dsb

Republik Österreich

Datenschutz behörde

Datenschutzbericht 2017

Datenschutzbericht 2017

Wien, im März 2018

Impressum

Medieninhaber, Herausgeber und Redaktion:
Datenschutzbehörde, Dr. Andrea Jelinek
(gemäß § 35ff DSG 2000), Wickenburggasse 8, 1080 Wien
Kontakt: dsb@dsb.gv.at
Website: www.dsb.gv.at
Fotonachweis: Kozhera (Seite 5)
Gestaltung: Datenschutzbehörde
Druck: BMVRDJ
Wien, 2018

Inhalt

1 Vorwort

Die unabhängige Datenschutzbehörde (DSB) ist seit 1. Jänner 2014 die nationale Kontrollstelle im Sinne des Art. 28 der Datenschutzrichtlinie 95/46/EG und wird ab 25. Mai 2018 diese Aufgabe aufgrund § 18 Datenschutzgesetz (iVm Art. 51 DSGVO) wahrnehmen. Zu ihren Aufgaben zählt die Führung von Individualverfahren auf Antrag des Stammzahlenregisters. Zudem führt die DSB amtswegige datenschutzrechtliche Überprüfungen durch und ist als aktives Mitglied in zahlreichen internationalen und nationalen Gremien präsent.

Die Arbeit der Datenschutzbehörde war im Jahr 2017 - neben der täglichen Arbeit – geprägt von der Vorbereitung auf die Geltung der DSGVO ab 25. Mai 2018. Die Mitarbeiterinnen und Mitarbeiter der Datenschutzbehörde haben im Jahr 2017 sowohl national als auch international mehr als 50 Vorträge gehalten, haben unzählige Veranstaltungen besucht, haben an einem Kommentar an der DSGVO mitgeschrieben und sich durch die Erweiterung ihrer Sprachkompetenz auf die Arbeit mit der DSGVO vorbereitet. Die Wichtigkeit des Grundrechts auf Datenschutz wird durch die DSGVO unterstrichen und die Aufgabe der europäischen Datenschutzbehörden wird es sein, die einheitliche Anwendung der Verordnung in der europäischen Union zu gewährleisten.

Der Datenschutzbericht 2017 ist der vierte, gemäß § 37 Abs. 5 DSG 2000, jährlich zu erstellende Bericht über die Tätigkeit der Datenschutzbehörde, der dem Bundesminister für Verfassung, Reformen, Delegierung und Justiz bis 31. März des Folgejahres zu übergeben und in geeigneter Weise durch die Behörde zu veröffentlichen ist. Die Veröffentlichung wird auf der Homepage der Datenschutzbehörde erfolgen.

Interessierte können sich auch während des Jahres über die Tätigkeiten der Datenschutzbehörde informieren; der seit 01/2015 quartalsmäßig erscheinende Newsletter der DSB gibt einen guten Überblick über Neuerungen, Judikatur und sonstige interessante Bereiche aus der nationalen und internationalen Welt des Datenschutzes.

Die Datenschutzbehörde stellt einen - durchaus auch für Nichtjuristinnen und Nichtjuristen konzipierten - Leitfaden zur DSGVO auf ihrer Website zur Verfügung, der regelmäßig aktualisiert wird.

Dr. Andrea Jelinek
Leiterin der Datenschutzbehörde

2 Die Datenschutzbehörde

2.1 Organisation und Aufgaben

2.1.1 Die Datenschutzbehörde

Die Datenschutzbehörde ist monokratisch strukturiert, aufgrund europarechtlicher und völkerrechtlicher Vorgaben unabhängig und keiner Dienst- und Fachaufsicht unterworfen.

Die Leiterin der Datenschutzbehörde ist Dr. Andrea Jelinek, der stellvertretende Leiter Dr. Matthias Schmidl. Beide wurden vom Bundespräsidenten auf Vorschlag der Bundesregierung mit 1. Jänner 2014 für die Dauer von fünf Jahren bestellt. Wiederbestellungen sind zulässig.

2.1.2 Aufgaben

Die Datenschutzbehörde ist insbesondere zuständig für die Behandlung von Eingaben von Personen, die sich durch Tätigkeiten eines Dritten (z.B. Unternehmer, Nachbar, Behörde etc.) in datenschutzrechtlichen Rechten (Geheimhaltung, Auskunft, Richtigstellung, Löschung) verletzt erachten.

Im Rahmen eines antragsbedürftigen Beschwerdeverfahrens nach § 31 DSG 2000 kann die Datenschutzbehörde eine Rechtsverletzung mit Bescheid feststellen.

Das Kontroll- und Ombudsmannverfahren nach § 30 DSG 2000 ist ein Verfahren, das auf die Herstellung des rechtmäßigen Zustandes abzielt und entweder auf Antrag oder von Amts wegen geführt wird. Dieses Verfahren ist im Bereich des soft law angesiedelt und hat mediativen Charakter. Die Datenschutzbehörde kann gegebenenfalls Empfehlungen aussprechen und veröffentlichen. Bescheide können in diesem Verfahren, abgesehen von Mandatsbescheiden nach § 30 Abs. 6a DSG 2000, nicht erlassen werden.

Die Datenschutzbehörde hat die Verwendung von Daten für wissenschaftliche Forschung und Statistik oder die Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen (§§ 46 und 47 DSG 2000) in bestimmten Fällen mit Bescheid zu genehmigen.

Darüber hinaus genehmigt die Datenschutzbehörde, in bestimmten Fällen den Transfer von Daten in Drittländer mit Bescheid (§ 13 DSG 2000).

Die zahlenmäßig umfangreichste Aufgabe der Datenschutzbehörde besteht in der Erteilung von Rechtsauskünften an Bürgerinnen und Bürger. Die Datenschutzbehörde kann jedoch nur insoweit Rechtsauskünfte erteilen, als damit nicht eine allfällige Entscheidung in einem konkreten Beschwerde-, Kontroll- oder Registrierungsverfahren vorweggenommen wird. Im Regelfall kann daher nur abstrakt und nicht fallbezogen eine Rechtsauskunft erteilt werden.

Darüber hinaus führt die Datenschutzbehörde das Datenverarbeitungsregister. Grundsätzlich ist eine Datenanwendung vor Inbetriebnahme vom jeweiligen Auftraggeber dem Datenverarbeitungsregister zu melden (§§ 17 ff DSG 2000). Die Datenschutzgrundverordnung kennt ab 25.05.2018 kein Register mehr (beachte jedoch: Datenschutzfolgenabschätzung in der Verantwortung des jeweiligen datenschutzrechtlich Verantwortlichen). Zu diesem Zeitpunkt anhängige Verfahren werden eingestellt, das Datenverarbeitungsregister ist von der Datenschutzbehörde bis 31.12.2019 zu Archivzwecken zuführen. Registrierungen im DVR werden gegenstandslos (§69 Abs. 2 DSG).

Alle Bescheide der Datenschutzbehörde können mit Beschwerde an das Bundesverwaltungsgericht bekämpft werden. Dieses entscheidet im Dreiersenat (ein Berufsrichter, zwei Laienrichter).

Entscheidungen des Bundesverwaltungsgerichtes können – auch von der Datenschutzbehörde – mit Revision an den Verwaltungsgerichtshof bzw. Beschwerde an den Verfassungsgerichtshof bekämpft werden.

Das E-Government-Gesetz überträgt der Datenschutzbehörde die Funktion der Stammzahlenregisterbehörde. In diesem Kontext obliegen der Datenschutzbehörde auch die Führung des Ergänzungsregisters sowie die Errechnung von Stammzahlen.

Darüber hinaus ist die Datenschutzbehörde in internationalen Foren auf EU-Ebene sowie des Europarates vertreten und arbeitet mit ihren Partnerbehörden eng zusammen.

Die Datenschutzbehörde stellt auf der Website der DSB (https://www.dsb.gv.at/rechte-der-betroffenen) allgemeine Informationen zu den Verfahren vor der Datenschutzbehörde sowie Musterformulare für Eingaben zur Verfügung.

Informationen zum Meldeverfahren werden auf der Webseite der DSB (https://www.dsb.gv.at/zugang-zu-dvr-online) bereitgestellt.

Die Entscheidungen der Datenschutzbehörde werden nur dann im RIS veröffentlicht, wenn sie von der Rechtssprechung der ehemaligen Datenschutzkommission abweichen, es keine Rechtsprechung der Datenschutzkommission zu einer Rechtsfrage gibt oder diese Rechtsprechung uneinheitlich ist. Die Veröffentlichung erfolgt grundsätzlich dann, wenn keine Anfechtung vor dem Bundesverwaltungsgericht erfolgt.

2.2 Der Personalstand

Im Berichtszeitraum versahen 27 Personen in Teil- oder Vollzeit ihren Dienst bei der Datenschutzbehörde, davon 15 Juristinnen und Juristen (davon ein Praktikant, eine geringfügig Beschäftigte), 4 Mitarbeiterinnen im gehobenen Dienst und 8 Mitarbeiterinnen und Mitarbeiter im Fachdienst. Die Bediensteten der Datenschutzbehörde sind in Erfüllung ihrer Aufgaben an die Weisungen der Leitung gebunden.

Die Vorbereitungen auf die Datenschutzgrundverordnung (siehe auch Punkt 5 des Berichts) zeigen deutlich, dass die Datenschutzbehörde mit 2018 jedenfalls – wie alle anderen Datenschutzbehörden in Europa auch – zusätzlichen Personalbedarf hat.

Der Behörde wachsen neue Aufgaben zu, deren Erfüllung nicht durch den Wegfall des Datenverarbeitungsregisters (und der Arbeit in diesem Bereich) kompensiert werden kann.

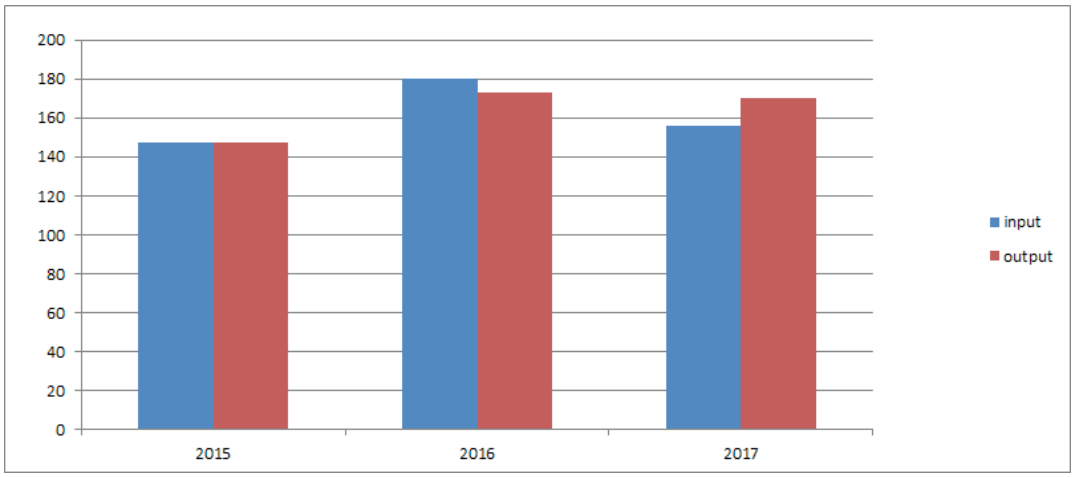
3 Tätigkeit der Datenschutzbehörde

3.1 Statistische Darstellung

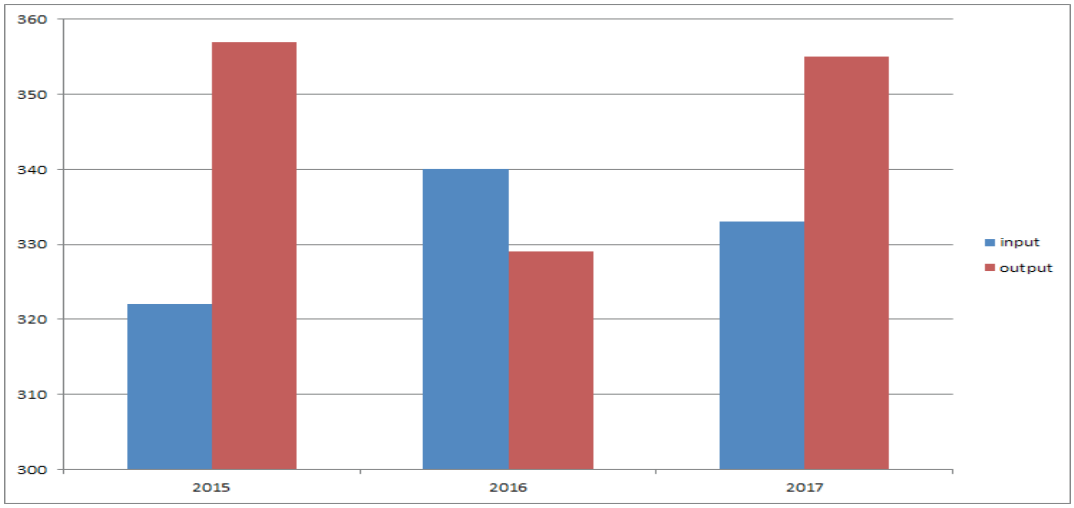
Tabelle 1 Anzahl der Eingangsstücke und Erledigungen

	Eingangsstücke			Erledigungen		
Art der Tätigkeit	**2015**	**2016**	**2017**	**2015**	**2016**	**2017**
Individualbeschwerden	147	180	156	147	173	170
Erledigungsart der Individualbeschwerden	147	173	170	95 Bescheide 52 Einstellungen	122 Bescheide 51 Einstellungen	115 Bescheide 55 Einstellungen
Kontroll- Ombudsmannverfahren nach § 30 DSG 2000 (Verfahren über Antrag)	332	340	333	357	329	355
Kontroll- Ombudsmannverfahren nach § 30 DSG 2000 (amtswegiges Prüfverfahren)	67	90	93	97	80	106
Rechtsauskünfte	2152	2004	2239	2123	1980	2192
Genehmigungen nach § 46 und 47 DSG 2000 (wissenschaftliche Forschung u Statistik)	16	23	19	18	18	19
Genehmigungen im Internationalen Datenverkehr	128	312	185	150	254	201
Auskunft Schengen	10	20	15	7	20	15
Verfahren vor dem Bundesverwaltungsgericht	31	34	33			

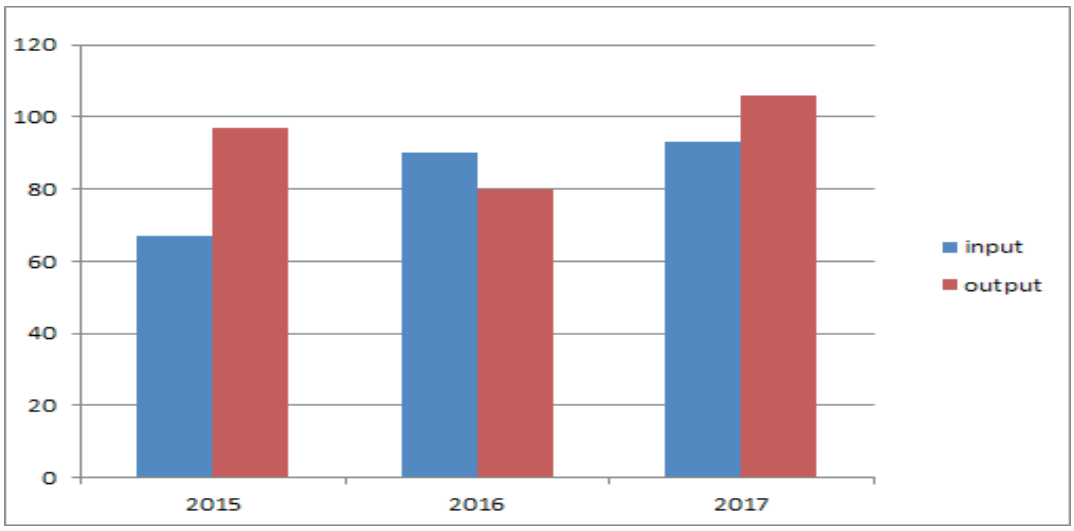
Individualbeschwerden § 31 DSG 2000



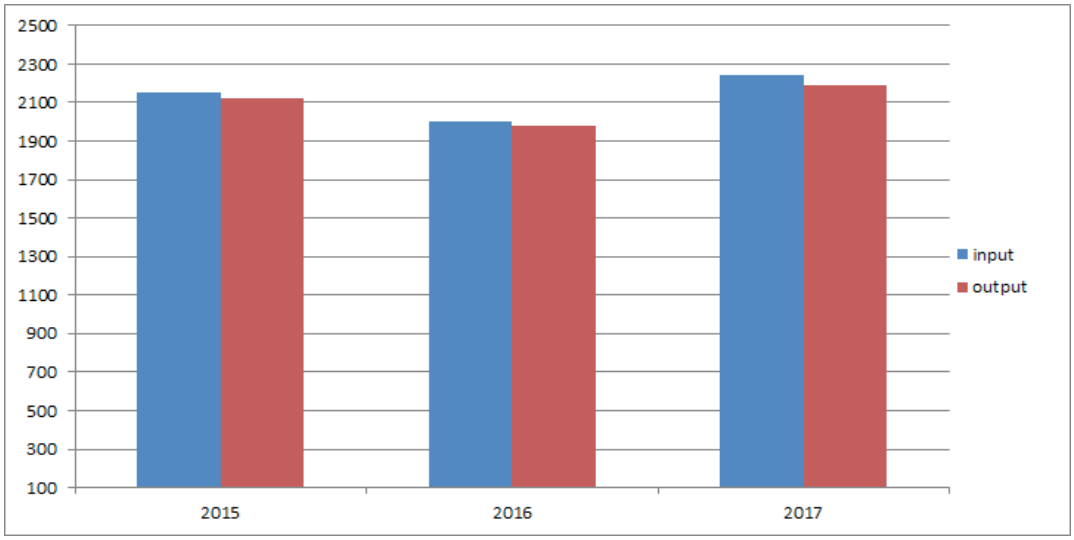
Kontroll- und Ombudsmannverfahren (§ 30 DSG 2000)



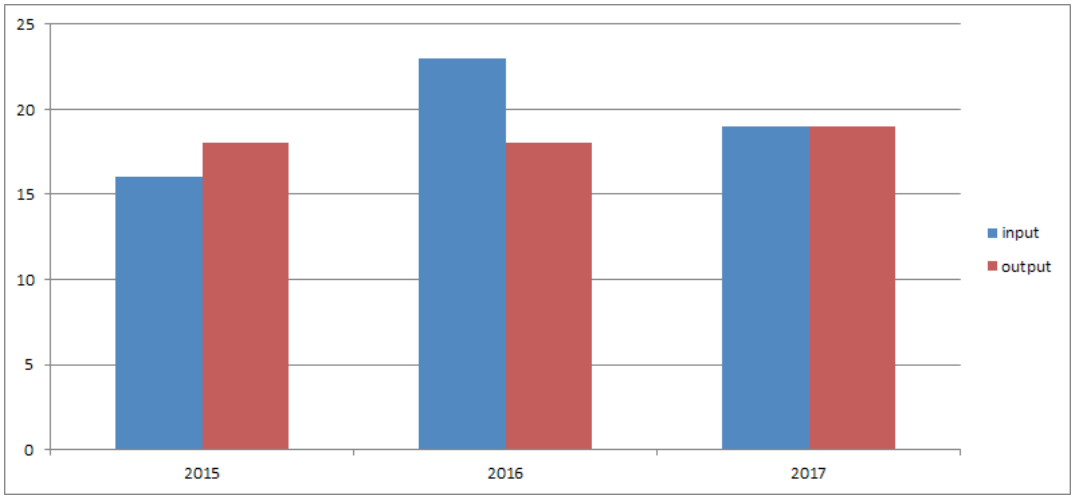
Amtswegiges Prüfverfahren (§ 30 Abs. 2 DSG 2000)



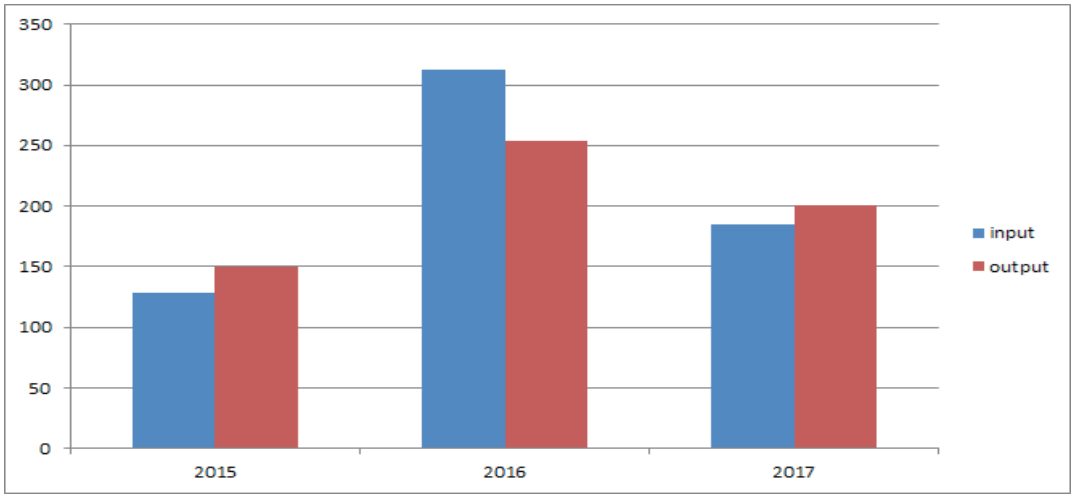
Rechtsauskünfte



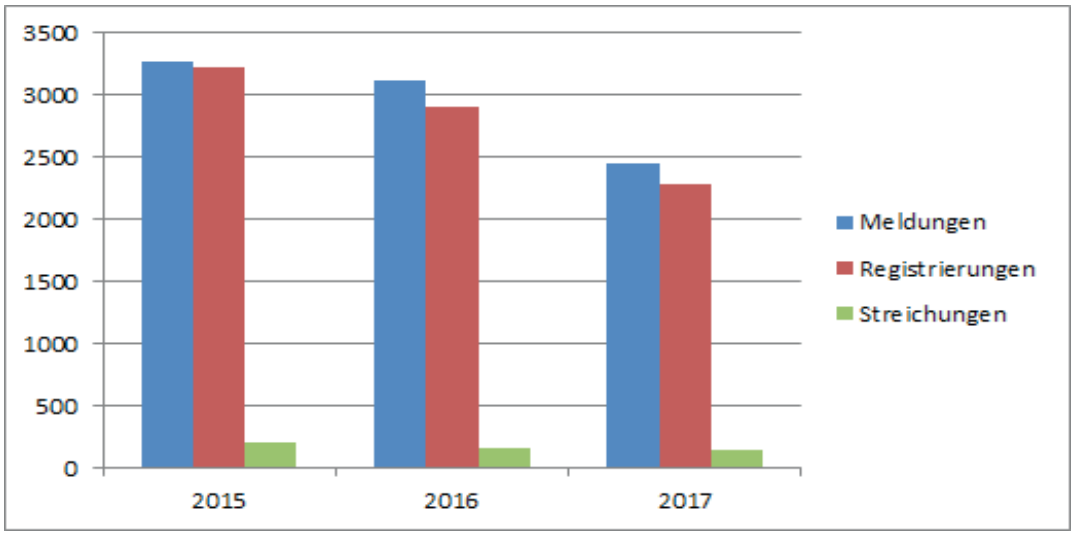
Genehmigung nach § 46 und 47 DSG 2000



Genehmigung im Internationalen Datenverkehr (§§ 12 und 13 DSG 2000)



Auftraggeber



Datenanwendungen

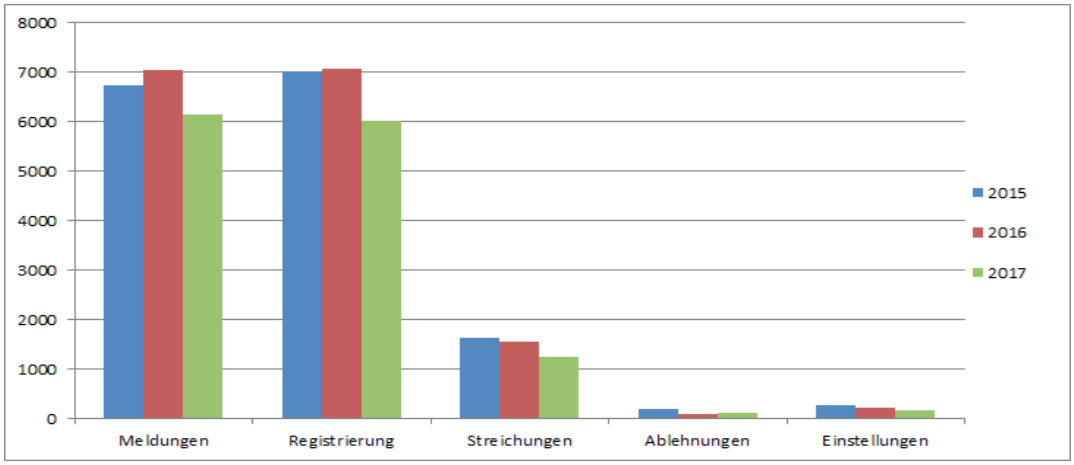


Tabelle 2 Anzahl der Tätigkeiten des Datenverarbeitungsregisters

Tätigkeiten	2015	2016	2017
Tätigkeiten für Auftraggeber in Summe	**6703**	**6186**	**4898**
Meldungen	3276	3119	2455
Registrierungen	3226	2901	2290
davon automatisch registriert	*2365 (ca. 73 %)*	*2135 (ca. 73 %)*	*1540 (ca. 67 %)*
davon durch das DVR registriert	*861 (ca. 27 %)*	*766 (ca. 27 %)*	*750 (ca. 33 %)*
Streichungen	201	166	153
Tätigkeiten in Datenanwendungen in Summe	**15872**	**16007**	**13703**
Meldungen	6741	7045	6154
davon automatisch registriert	*3985 (ca. 59 %)*	*4300 (ca. 61 %)*	*3432 (ca. 56 %)*
davon vom DVR überprüft	*2756 (ca. 41 %)*	*2745 (ca. 39 %)*	*2722 (ca. 44 %)*
Registrierungen	7028	7072	6016
Streichungen	1633	1558	1239
Ablehnungen	191	105	115
Einstellungen	279	227	179
Verbesserungsaufträge in Summe	**1073**	**1009**	**1000**
Bescheide im Registrierungsverfahren	8	3	1
Verfahren gemäß § 22a DSG 2000	9	2	8
Rechtsunwirksam eingebrachte Meldungen	112	104	96
Meldungen von Rechtsnachfolgen	44	57	91

3.2 Verfahren und Auskünfte

3.2.1 Individualbeschwerden

Allgemeines und Grundsätzliches

Das Beschwerdeverfahren nach § 31 DSG 2000 war bisher das wichtigste Rechtsschutzverfahren im Zuständigkeitsbereich der DSB. Das Jahr 2017 ist das letzte vollständige Berichtsjahr, in dem aus dem nationalen Datenschutzrecht ableitbare subjektive Rechte in diesem Verfahren durchzusetzen waren.

Beschwerden wegen Verletzung der Rechte auf Auskunft, Geheimhaltung, Löschung oder Richtigstellung (§ 31 Abs. 2 DSG 2000) sind gegen alle datenschutzrechtlichen Auftraggeber der öffentlichen Verwaltung möglich; gegen Auftraggeber aus dem privaten Bereich sind nur Beschwerden wegen Verletzung des Rechts auf Auskunft (§ 31 Abs. 1 DSG 2000) zulässig. Gesetzgebung (samt zugeordneten Prüforganen wie Rechnungshof und Volksanwaltschaft) und Gerichtsbarkeit (ausgenommen die monokratische, d.h. nicht durch richterliche Kollegien ausgeübte Justizverwaltung) sind von der Zuständigkeit der DSB ausgenommen.

Der inhaltliche Schwerpunkt im österreichischen datenschutzrechtlichen Beschwerdeverfahren liegt somit bei Themen aus dem Bereich der innerstaatlichen öffentlichen Verwaltung und bei der Auskunftserteilung durch private Rechtsträger.

Formell handelt es sich um ein Verwaltungsverfahren nach dem Allgemeinen Verwaltungsverfahrensgesetz 1991 (AVG).

Die Beschwerde gemäß § 31 DSG 2000 ist ein förmlicher Rechtsschutzantrag an die DSB.

Inhaltlich handelt es sich regelmäßig um ein Zweiparteienverfahren, in dem die Seiten gegensätzliche Standpunkte vertreten (= kontradiktorisches Verfahren). Die Parteien werden als Beschwerdeführer und Beschwerdegegner bezeichnet.

Der DSB kommt von Gesetzes wegen hier die Rolle einer unabhängigen Streitentscheidungsinstanz zu (§ 31 Abs. 1, 2 und 7, § 37 Abs. 1 DSG 2000). Die Entscheidungen im Verfahren werden durch die Leiterin der DSB oder in ihrem Namen durch ihren Stellvertreter oder einen aufgrund einer Ermächtigung handelnden Vertreter („Genehmiger“) getroffen. Die ermächtigten Vertreter sind an allfällige Weisungen der Leiterin gebunden.

Im Verfahren wegen Verletzung der Rechte auf Auskunft, Löschung oder Richtigstellung muss dem Beschwerdeverfahren vor der DSB zwingend ein „Vorverfahren“ zwischen Betroffenem und Auftraggeber vorangegangen sein, in dem ersterer das jeweilige Recht geltend gemacht hat. Dieser Schriftwechsel muss der DSB vorgelegt werden (§ 31 Abs. 4 DSG 2000). Ein Fehlen des entsprechenden Nachweises wird als Inhaltsmangel behandelt, der bei Nichtbehebung zur Zurückweisung der Beschwerde durch Bescheid führt.

Werden die Rechte auf Auskunft, Löschung oder Richtigstellung vom Betroffenen gegenüber einer Verwaltungsbehörde oder einem anderen datenschutzrechtlich Verantwortlichen (Auftraggeber) des öffentlichen Bereichs geltend gemacht, so ist eine Behörde, unabhängig von der Bezeichnung des Anbringens („Antrag auf Richtigstellung von Daten“) nicht verpflichtet und auch nicht berechtigt, die Sache durch einen Bescheid zu erledigen. In jedem Fall muss aber eine Mitteilung ergehen. Diese, bis auf die Schriftlichkeit nicht formgebundene Mitteilung

des Auftraggebers ist im Anschluss gegebenenfalls im Beschwerdeverfahren von der DSB zu überprüfen. Die verwaltungsgerichtliche Kontrolle beginnt erst nach einem Zwischenschritt in Form eines Bescheids der DSB. Dieses Abweichen von dem in Art. 130 Abs. 2 Z 1 des Bundesverfassungsgesetzes angelegten System ist durch Unionsrecht bedingt (Art. 28 der Richtlinie 95/46/EG; Garantie des Bestehens einer unabhängigen Kontrollstelle für Datenschutz in Art. 8 Abs. 2 der Charta der Grundrechte der EU).

Praxis der Beschwerdeverfahren im Jahr 2017

Das Berichtsjahr ist ohne auffällige Entwicklungen insbesondere Häufung von Beschwerdeverfahren mit gleichem oder ähnlichem Gegenstand verlaufen. Statistisch ist die Zahl der angefallenen Beschwerden gesunken, siehe Kapitel Statistik.

Im Berichtsjahr verteilten sich die dokumentierten Beschwerdeverfahren ziemlich gleichmäßig auf die Rechte auf Geheimhaltung, Richtigstellung/Löschung und Auskunft, insbesondere, wenn man in Rechnung stellt, dass letzteres Recht auf Grund des erweiterten Zuständigkeitsbereichs der DSB statistisch praktisch immer an der Spitze liegen würde.

Wie bereits für das Jahr 2016 berichtet, waren auch 2017 immer wieder Fälle zu beobachten, in denen insbesondere das Recht auf Auskunft und die daran anknüpfenden Rechtschutzverfahren erkennbar dazu verwendet worden sind, aus abseits der Sorge um das Grundrecht auf Datenschutz liegenden Motiven, verschiedene Auftraggeber in Verfahren und Rechtsstreitigkeiten zu verwickeln. Da das Recht auf Auskunft als Kontrollrecht jedoch ohne Offenlegung eines Grundes ausgeübt werden kann, ist ein solches Vorgehen rechtmäßig, solange es nicht ausschließlich in der Absicht erfolgt, dem Auftraggeber Nachteile zuzufügen (= Schikane). Nachgewiesene Fälle von Schikanen im Beschwerdeverfahren liegen der DSB bis heute nicht vor, es wurde dies aber von unterlegenen Auftraggebern (=Verantwortlicher) mehrfach in Beschwerden vor dem Bundesverwaltungsgericht behauptet und gegen das Bestehen eines Rechts auf Auskunft eingewendet. Das Bundesverwaltungsgericht hat sich zu dieser Frage im Berichtszeitraum noch nicht geäußert.

Bisher hat die DSB in solchen Fällen auf die Kostenersatzpflicht gemäß § 26 Abs. 6 DSG 2000 hingewiesen (Anspruch auf Erhalt einer kostenlosen Auskunft über eigene Daten auf einmalige Ausübung des Rechts pro Kalenderjahr beschränkt). Diese Bestimmung tritt mit der Anwendbarkeit der DSGVO außer Kraft. In Zukunft könnten solche Fälle nach Art. 15 Abs. 3 (Anspruch des Auskunftspflichtigen auf ein Entgelt für „weitere Kopien“ der Daten des Betroffenen) und Art. 57 Abs. 4 DSGVO zu beurteilen sein (Kostenersatzpflicht bei „offenkundig unbegründeten“ oder „exzessiven“ Anbringen an die DSB).

Die durch die DSG-Novelle 2010 eingeführte Möglichkeit, Beschwerdeverfahren als „gegenstandslos“ durch Einstellung zu beenden (§ 31 Abs. 8 DSG 2000), hat sich auch im Jahr 2017 als wesentlich für die Arbeit der DSB erwiesen. Die Bestimmung ist inhaltlich ins DSG übernommen worden. Sie ermöglicht es insbesondere, Beschwerdeverfahren wegen Auskunfts- oder Löschungsverlangen, auf die der Auftraggeber in gesetzwidriger Weise zunächst nicht reagiert hat, nach Erreichung des primären Verfahrensziels (Beantwortung des Auskunfts- oder Löschungsverlangens) ohne großen Aufwand zu beenden. Im Jahr 2017 konnte rund ein Drittel der verfahrensbeendenden Erledigungen im Beschwerdeverfahren als Einstellung ergehen (55 von 170, Beschwerdezurückziehungen aus anderen Gründen eingeschlossen) werden. Die Praxis dieser Form der Verfahrensbeendigung wegen Klaglosstellung wurde inzwischen mehrfach durch das Bundesverwaltungsgericht als rechtmäßig bestätigt.

Ausgewählte Beschwerdeentscheidungen aus 2017

Die Datenschutzbehörde hat in ihrer öffentlich zugänglichen Entscheidungsdokumentation (im Rahmen des Rechtsinformationssystems des Bundes – RIS; Stand: 22. Jänner 2018) aus dem Jahr 2017 fünf Bescheide aus Beschwerdeverfahren dokumentiert. Diese Zahl kann sich aus verschiedenen Gründen (z.B. wegen abzuwartender Rechtsmittelentscheidungen des BVwG, VfGH oder VwGH) auch nach Erscheinen des Datenschutzberichts 2017 noch ändern.

Über andere Entscheidungen wurde im Newsletter der DSB berichtet.

Regelmäßig werden nur rechtskräftige Entscheidungen dokumentiert, Ausnahmefälle sind in den RIS-Dokumenten durch entsprechende Vermerke gekennzeichnet. In solchen Fällen wird die Entscheidung nach einer Aufhebung durch das Bundesverwaltungsgericht aus dem RIS entfernt oder der sonstige Ausgang des Verfahrens dokumentiert.

Die wichtigsten Beschwerdeentscheidungen in chronologischer Reihenfolge:

a. Bescheid vom 27.3.2017, GZ: DSB-D122.616/0006-DSB/2016 (Auskunft über Standortdaten an den Vertragsinhaber)

In dieser Entscheidung setzt sich die DSB mit der Frage auseinander, ob ein Vertragsinhaber bei seinem Mobilfunkanbieter Standortdaten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers angeben, im Rahmen des Auskunftsrechts erfragen darf. Da die Standortdaten als betriebstechnisch notwendige Daten zum „Routing“ innerhalb des Kommunikationsnetzes – also letztlich im Rahmen der Diensteerbringung (z.B. Telefonieren, SMS) bei mobilen Endgeräten – erforderlich sind, kann die Entstehung dieser Standortdaten vom Nutzer nicht verhindert/beendet oder ausgeschaltet werden, wie dies etwa bei einigen Apps, die über die GPS-Funktion des Smartphone eine Standortverfolgung ermöglichen, der Fall ist. Der Beschwerdeführer legte eine eidesstättige Erklärung vor, in der er darlegte Eigentümer und einzig Verfügungsbefugter für Gerät und Vertrag zu sein. Der Mobilfunkanbieter verweigerte dem Vertragsinhaber die Daten zu beauskunften. Dies wurde damit begründet, dass aufgrund des Telekommunikationsgesetzes (TKG 2003), als spezialgesetzliche Norm, Standortdaten ausschließlich im Zuge polizeilicher Ermittlungen oder richterlicher Anordnungen bzw. den Betreibern von Notrufdiensten, wenn ein Notfall dadurch abgewehrt werden kann, übermittelt werden dürften. Die DSB folgte im Ergebnis dem Mobilfunkanbieter und sprach aus, dass die Einschränkung des Auskunftsrechts durch die Rechtsprechung des OGH gedeckt ist, wonach aufgrund des TKG 2003 dem Betroffenen nur ein auf Erhalt eines Einzelentgeltnachweises eingeschränktes Recht, über gespeicherte Verkehrsdaten Auskunft zu erhalten, einzuräumen ist. Im konkreten Fall war somit der Einschränkung der Auskunftserteilung im Rahmen der spezialgesetzlichen Bestimmung des TKG 2003 der Vorzug gegenüber dem in § 26 Abs. 1 DSG 2000 festgelegten allgemeinen Recht auf Auskunft des Beschwerdeführers zu geben.

b. Bescheid vom 7.4.2017, GZ: DSB-D122.671/0007-DSB/2017 (Auskunft über Mitarbeiter des Auftraggebers, Newsletter 3/2017, nicht rechtskräftig)

In dieser Sache hatte die DSB die Frage zu beurteilen, ob das Auskunftsrecht auch die Benennung konkreter Mitarbeiter eines Auftraggebers umfasst. Die Beschwerdeführerin hatte eine allgemeine Auskunft darüber verlangt, welche Mitarbeiter des Auftraggebers ihre Daten in einem bestimmten Zeitraum abgefragt hatten. Unter Verweis auf die Rechtsprechung der Datenschutzkommission hielt die DSB zunächst fest, dass das Auskunftsrecht nur Übermittlungsvorgänge an neue Auftraggeber umfasst, nicht aber einzelne Datenverarbeitungen von Mitar-

beitern des Auftraggebers. Die Namen von Mitarbeitern des Auftraggebers sind auch nicht „zur Person des Auskunftswerbers verarbeitete Daten“ oder „verfügbare Informationen über ihre Herkunft“, weshalb diese auch nicht von § 26 DSG 2000 umfasst sind. Darüber hinaus soll das Auskunftsrecht dem Auskunftswerber helfen, sein Recht auf Geheimhaltung und sein Recht auf Löschung zu sichern. Diese Rechte richten sich jedoch gegen den jeweiligen Auftraggeber und nicht gegen den jeweiligen Mitarbeiter. Die DSB erkannte allerdings auch, dass die Benennung konkreter Mitarbeiter eines Auftraggebers dann vom Auskunftsrecht umfasst ist, wenn der Betroffene hinreichend konkrete Hinweise hat, dass er von einem Mitarbeiter des Auftraggebers in seinen datenschutzrechtlichen Rechten verletzt worden ist. Der Auskunftswerber muss dies aber bereits im Auskunftsbegehren klar zum Ausdruck bringen, damit der Auftraggeber abwägen kann, ob das Recht des Betroffenen auf Auskunft oder das Recht des Mitarbeiters auf Geheimhaltung höher zu bewerten ist. Da die Beschwerdeführerin im gegenständlichen Fall keinen konkreten Verdacht äußerte, wurde die Beschwerde abgewiesen. Gegen diesen Bescheid ist Beschwerde an das BVwG erhoben worden.

c. Bescheid vom 30.5.2017, GZ: DSB-D122.640/0001-DSB/2017 (Übermittlung von Wählerdaten an politische Parteien und Kandidaten)

In dieser Sache hatte sich die DSB mit der Beschwerde eines Auslandsösterreichers zu befassen, der im Wahlkampf für die Bundespräsidentenwahlen 2016 einen Werbebrief und eine E-Mail eines der Kandidaten erhalten hatte. Die Wählerevidenzbehörde (Stadtgemeinde), gegen die Beschwerde geführt wurde, hatte seine Kontaktdaten, zu denen bei Auslandsösterreichern, wie im Fall des Beschwerdeführers, auch eine freiwillig bekannt gegebene E-Mail gehören kann, an das Bundesministerium für Inneres (BMI) für Zwecke der dort geführten Zentralen Wählerevidenz übermittelt, von wo sie gesetzmäßig an alle im Nationalrat vertretenen politischen Parteien gelangten (§ 3 Abs. 5 Wählerevidenzgesetz - WEvG). Für letztere Übermittlungen war jedoch das BMI verantwortlich. Die ebenfalls erfolgte Übermittlung der Daten des Wählerverzeichnisses an den Zustellbevollmächtigten des betreffenden Kandidaten war ebenfalls gesetzlich vorgesehen. Die DSB hielt fest, dass der Kandidat bzw. die diesen unterstützende politische Partei diese Daten zur Versendung von Wahlwerbung benutzen durfte. Die Beschwerde wurde daher abgewiesen.

d. Bescheid vom 8.6.2017, GZ: DSB-D122.641/0006-DSB/2017 (Auskunft über Bonitätsprüfung eines Zahlers)

In diesem Bescheid hatte sich die DSB mit einer Frage der datenschutzrechtlichen Auskunftserteilung über Bonitätsdaten zu befassen. Der Beschwerdeführer bezahlte im Lastschriftverfahren die von einem Dritten zu leistenden Entgelte für die Dienste eines Mobilfunkunternehmens (Beschwerdegegnerin). Anlässlich einer Änderung des Lastschriftmandats (anderes Bankkonto) kam es zu einem fehlgeschlagenen Geldeinzug, Reklamationen und in weiterer Folge zur Einholung von Bonitätsauskünften über den Beschwerdeführer durch die Beschwerdegegnerin bei einem Wirtschaftsauskunftsdienst. Danach forderte die Beschwerdegegnerin den Beschwerdeführer zur Erbringung eines Identitäts- und Einkommensnachweises auf. Dieser antwortete, anwaltlich vertreten, mit einem datenschutzrechtlichen Auskunftsverlangen. Die Beschwerdegegnerin verneinte zunächst die Durchführung einer „Bonitätsabfrage“ zu Gänze, ergänzte die Auskunft aber schließlich im bereits laufenden Beschwerdeverfahren dahingehend, dass „negative“ Bonitätsauskünfte „vermerkt“ worden seien. Damit gab sich der Beschwerdeführer jedoch nicht zufrieden. Das Ermittlungsverfahren, in dem u.a. eine verantwortliche Mitarbeiterin der Beschwerdegegnerin als Zeugin befragt wurde, ergab, dass das Ergebnis der Bonitätsprüfung (nach dem Ampelsystem grün-gelb-rot) im CRM-System (Kundenbetreuungssystem) gespeichert wurde. Außerdem war über den Wirtschaftsauskunftsdienst

(als Dienstleister) nicht korrekt Auskunft erteilt worden (Angabe der Firma einer Holding anstatt jener der operativen Tochtergesellschaft). Die DSB gab daher der Beschwerde teilweise Folge und trug der Beschwerdegegnerin auf, eine inhaltliche Auskunft über die verarbeiteten Bonitätsdaten und eine korrekte Auskunft über die Firma des Dienstleisters zu geben. Die DSB betonte dabei, dass bei gespeicherten Bonitätsdaten ein berechtigtes Interesse des Betroffenen besteht, den genauen Inhalt dieser Daten zu erfahren.

Hinsichtlich eines Auskunftsverlangens zur Logik der automatisierten Entscheidungsfindung der Bonitätsprüfung (§ 49 DSG 2000) wurde der Beschwerdeführer hingegen von der Beschwerdegegnerin zu Recht an den Wirtschaftsauskunftsdienst verwiesen, da die Beschwerdegegnerin nicht für die im „Ampelsignal" ausgedrückte Bonitätsbeurteilung sondern nur für daran anknüpfende wirtschaftliche Entscheidungen verantwortlich war.

e. Bescheid vom 16.10.2017, GZ: DSB-D122.689/0006-DSB/2017 (Löschung erkennungsdienstlicher Daten, Gefährlichkeitsprognose)

Die Beschwerdeführerin (und ihr Ehemann) wurde u.a. mehrerer Sexualdelikte an Minderjährigen beschuldigt. Sie wurde nicht verurteilt, die Strafsache wurde nach mehreren Rechtsmitteln durch Einstellung oder Freispruch rechtskräftig beendet, da bereits Verjährung eingetreten war. Die Beschwerdeführerin verlangte daraufhin die Löschung der sie betreffend verarbeiteten erkennungsdienstlichen Daten (insbesondere Fingerabdrücke und DNA-Daten). Dies wurde von der Sicherheitsbehörde mit der Begründung abgelehnt, die Strafsache sei nur aus formalen Gründen beendet worden, es liege aber eine „subjektiv positive Gefährdungsprognose" vor, wonach die Beschwerdeführerin auf Grund ihrer Persönlichkeit neuerlich einschlägige Straftaten begehen könnte, zu deren Prävention oder Aufklärung die weitere Datenverarbeitung erforderlich sei.

Die DSB hat die von der mit Beschwerde belangten Sicherheitsbehörde vorgenommene Interessenabwägung für zutreffend erachtet. Die Daten seien gemäß §§ 65 und 67 des Sicherheitspolizeigesetzes – SPG rechtmäßig ermittelt und verarbeitet worden. Eine amtswegige Löschung war nicht geboten, ein auf § 27 Abs. 1 und 4 DSG 2000 gestütztes Löschungsverlangen bleibe erfolglos. Ausschlaggebend in der Interessensabwägung war insbesondere „der Umstand, dass mit der […] erfolgten Erhebung der Anklage gegen die Beschwerdeführerin ein solch konkretisierter Verdacht der Verwirklichung des Tatbildes eines – an Unmündigen begangenen - Sexualdelikts bestand, dass mit einer gerichtlichen Verurteilung gerechnet werden konnte." Dies erlaube den Schluss, dass von der Beschwerdeführerin weiterhin eine Gefahr für die öffentliche Sicherheit ausgehe. Die Beschwerde wurde daher rechtskräftig abgewiesen.

f. Bescheid vom 8.11.2017, GZ: DSB-D122.718/0006-DSB/2017 (Auswertung von Telefondaten für dienstliche Kontrollmaßnahmen, Newsletter 1/2018)

In diesem Bescheid hatte sich die DSB mit einer Frage der Zulässigkeit von Kontrollmaßnahmen am Arbeitsplatz zu befassen. Der Beschwerdeführer, ein während des Beschwerdeverfahrens entlassener Vertragsbediensteter des Bundes (arbeitsgerichtlich angefochten), beschwerte sich über behauptete Eingriffe in sein Grundrecht auf Geheimhaltung durch Ermittlungen seiner Personalstelle, durch die der Verdacht pflichtwidrigen Verhaltens überprüft werden sollte. Für diesen Zweck wurden u.a. Einzelverbindungsnachweise für die Nebenstelle und das Diensthandy des Beschwerdeführers angefordert. Hinsichtlich der solcherart erfolgten Ermittlung von Daten zu (Sprach-) Telefonverbindungen war die Beschwerde teilweise erfolgreich, da der auch auf Vertragsbedienstete anzuwendende 2. Satz in § 79e Abs. 3 BDG 1979 „Telefonie" ausdrücklich von den gemäß Unterabschnitt 5a des BDG 1979 zulässigen dienstrechtlichen Kont-

rollmaßnahmen ausnimmt. Es fehlte daher an einer ausreichenden rechtlichen Grundlage für den Grundrechtseingriff. Die Ermittlung von Daten zu sonstigen Kommunikationsverbindungen, einschließlich SMS, war dagegen nach Ansicht der DSB rechtmäßig, da die erforderlichen dienstrechtlichen Voraussetzungen für Kontrollmaßnahmen hier gegeben waren. Der Bescheid ist rechtskräftig.

g. Bescheid vom 9.11.2017, GZ: DSB-D122.706/0005-DSB/2017 (Datenübermittlung für Kontrolltätigkeit der Volksanwaltschaft)

Der Beschwerdeführer war Patient und erhielt in der Ambulanz einer Krankenanstalt des Wiener Krankenanstaltenverbundes (KAV, datenschutzrechtlich für den KAV verantwortlich: der Magistrat der Stadt Wien) Infusionen. Nach einem Vorfall in der betreffenden Ambulanz beschwerte sich der Beschwerdeführer bei der Volksanwaltschaft (VA) und behauptete einen Missstand in der Verwaltung. In seiner Stellungnahme an die VA erwähnte der Magistrat der Stadt Wien auch die Bezeichnung der verabreichten Infusion, was, unbestritten, Rückschlüsse auf die Erkrankung des Beschwerdeführers zulässt. Der Beschwerdeführer erhob nun auch Beschwerde an die DSB und behauptete darin eine Verletzung seines Rechts auf Geheimhaltung.

Die DSB hat die Beschwerde abgewiesen und dies mit ihrer ständigen „Denkmöglichkeitsjudikatur“ für Datenverwendung im Verwaltungsverfahren begründet, die sinngemäß auch auf Prüfverfahren der VA anzuwenden sei. Da der Beschwerdeführer gegenüber der VA auch eine Verletzung von Art. 3 EMRK behauptet hatte, war es denkmöglich, der VA alle Informationen zur Verfügung zu stellen, die zur Prüfung dieses Vorwurfs erforderlich waren. Die Art der Infusion diente in diesem Zusammenhang der Beurteilung der Frage, ob dem Beschwerdeführer eine lebensnotwendige, in keiner anderen Einrichtung mögliche Behandlung, verweigert worden war.

3.2.2 Kontroll- und Ombudsmannverfahren (§ 30 DSG 2000)

Im sogenannten Kontroll- und Ombudsmannverfahren gemäß § 30 DSG 2000 kann sich jedermann (Unternehmen, Behörde, Verein, Privatperson und so weiter) wegen einer behaupteten Verletzung seiner Rechte (zum Beispiel Auskunft, Löschung) oder ihn betreffender Pflichten (beispielsweise Meldung, Information) nach dem DSG 2000 mit einer Eingabe an die DSB wenden. Die Durchführung eines solchen weitestgehend formfreien Verfahrens ist (anders als beim Beschwerdeverfahren nach § 31 DSG 2000) unabhängig vom geltend gemachten Recht (Pflicht) bzw. dem angesprochenen datenschutzrechtlichen Auftraggeber zulässig, und zwar auch dann, wenn die Datenschutzbehörde alternativ auch zur förmlichen Rechtsdurchsetzung zuständig wäre. Ziel eines solchen Verfahrens ist nach § 30 Abs. 6 DSG 2000 die Herbeiführung des rechtmäßigen Zustands. Dazu kann die Datenschutzbehörde, falls erforderlich – nicht unmittelbar durchsetzbare – Empfehlungen aussprechen. Zumeist kann im Rahmen eines solchen Verfahrens eine datenschutzrechtlich zufriedenstellende Situation aber auch ohne Einsatz dieses Mittels erreicht werden.

Im Jahr 2017 betraf die zahlenmäßig größte Gruppe von Eingaben – nämlich eine Anzahl von 333 Eingangsstücken – wie bereits die Jahre zuvor die mediatisierenden Kontroll- und Ombudsmannverfahren, welche über Antrag eingeleitet wurden. Im Vergleich dazu wurden 93 Prüfungsverfahren amtswegig von der Datenschutzbehörde eingeleitet.

Im Berichtszeitraum scheinen die folgenden Fälle besonders erwähnenswert:

a. Empfehlung zur Verbindung der Annahme von AGBs für Abonnements mit der Zustimmung zur Datenverwendung für andere Zwecke (GZ: DSB-D216.396/0003-DSB/2017, 22. Mai 2017)

Der Einschreiter brachte vor, er habe bei der O***-Zeitungsverlag GmbH ein Testabonnement bestellt. Im Zuge der Bestellung habe er zwingend den AGB samt der in den AGB geregelten Verwendung seiner Daten zustimmen müssen. Ohne die Abgabe der Zustimmung zur Datenverwendung sei die Bestellung eines Abonnements nicht möglich gewesen. Die Datenschutzbehörde führte in ihrer Empfehlung aus, dass eine ausdrückliche Zustimmung des Betroffenen keinesfalls dann vorliegen kann, wenn sie bloß als Bestandteil von allgemeine Geschäftsbedingungen vom Betroffenen zur Kenntnis genommen wurde. Vielmehr liegt eine „ausdrückliche" schriftliche Zustimmung nur dann vor, wenn der Betroffene sein Einverständnis zur Datenübermittlung getrennt von etwaigen sonstigen vertraglichen Vereinbarungen gegeben hat. Hinsichtlich der Form der Zustimmungserklärung ist daher zu verlangen, dass diese deutlich vom übrigen Text eines Formulars, eines Schriftstückes udgl. abgesetzt ist. Im gegenständlichen Fall war es für den Einschreiter nicht möglich gewesen, den angestrebten Vertrag mit der O***-Zeitungsverlag GmbH zu schließen, ohne gleichzeitig die Zustimmungserklärung zur Datenverwendung für andere Zwecke als für die Abwicklung des Abonnements (v.a. für Kontaktaufnahme zu Werbezwecken) abzugeben. Dieser Umstand war nach Ansicht der Datenschutzbehörde mit dem Erfordernis der Freiwilligkeit iSd § 4 Z 14 DSG 2000 und § 8 Abs. 1 Z 2 DSG 2000 nicht vereinbar. Der Umstand, dass dem Kunden die Möglichkeit eingeräumt wird, die von ihm zunächst abgegebene Zustimmungserklärung jederzeit zu widerrufen, vermag an diesem Ergebnis nichts zu ändern. Die DSB empfahl daher die O***-Zeitungsverlag GmbH möge die Annahme der allgemeine Geschäftsbedingungen für Abonnements – und damit den Abschluss eines Vertrages – nicht mit der Zustimmung zur Datenverwendung für andere Zwecke verbinden bzw. von dieser abhängig machen.

b. Empfehlung zu einer Videoüberwachung (GZ: DSB-D216.405/0006-DSB/2017, 5. Dezember 2017)

Grundsätzlich orientiert sich die Befugnis zur Durchführung einer Videoüberwachung an der Verfügungsbefugnis eines privaten Auftraggebers über die im Einzelfall konkret zu überwachenden Örtlichkeiten. In Abgrenzung dazu sind an „öffentlichen Orten"– wie etwa öffentlichen Straßen – auf Grund des staatlichen Gewaltmonopols grundsätzlich nur die Sicherheitsbehörden zur Durchführung von Videoüberwachungen berechtigt. Im gegenständlichen Verfahren stellte sich somit zuerst die Vorfrage, ob es sich bei der Straße bzw. Verkehrsfläche am Privatgrundstück der Antragsgegnerin um eine Straße mit öffentlichem Verkehr handelt. Bereits am Schild zur Einfahrt zum gegenständlichen Grundstück war erkennbar, dass Kunden, Gäste und Mitarbeiter der Büros und Geschäftslokale die Straße uneingeschränkt benutzen können. Der berechtigte Personenkreis war somit unbestimmt, da am gegenständlichen Grundstück jedermann unter den gleichen Bedingungen die Möglichkeit besitzt, jedenfalls Gast bzw. Kunde der jeweiligen Unternehmungen zu werden. Da es sich um eine Verkehrsfläche bzw. Straße mit öffentlichem Verkehr handelte, waren die von der Antragsgegnerin ins Treffen geführten Voraussetzungen gemäß § 50a Abs. 4 DSG 2000 nicht mehr zu prüfen. Um sicherzustellen, dass eine Verletzung der schutzwürdigen Geheimhaltungsinteressen der Betroffenen (gegenständlich insbesondere Gäste, Kunden und Mitarbeiter) im Zuge des Einsatzes der Videoüberwachung ausgeschlossen werden konnte, empfahl die Datenschutzbehörde daher, dass die Kameras so ausgerichtet werden, dass entsprechend der bisherigen Spruchpraxis diese tatsächlich nur die gegenständlichen Bereiche (hier: Fassade und Eingänge der Gebäude am Grundstück) und den

sich unmittelbar davor befindlichen Bereich (maximal ca. 50 cm) erfassen, nicht jedoch den Gehsteig oder großräumige Flächen der Straße.

c. Empfehlung betreffend eine Videoüberwachung (GZ: DSB-D216.309/0007-DSB/2017, 22. November 2017)

Der Einschreiter und die Auftraggeberin waren je Eigentümer einer benachbarten Liegenschaft. Auf der Liegenschaft des Einschreiters befand sich ein LKW-Betrieb des Einschreiters. Dieses Transportunternehmen besaß auch eine Gewerbegenehmigung für den Betrieb eines Abstellplatzes auf dem Grundstück. Die Antragsgegnerin hatte im ersten Stock auf Höhe ihrer Betriebswohnung eine stationäre Videokamera installiert, die permanent auf das Nachbargrundstück des Einschreiters gerichtet war. Es wurden auf dem Abstellplatz unter anderem Mitarbeiter bzw. LKW-Fahrer und Kennzeichen von LKWs gefilmt. Die Antragsgegnerin begründete die Installation der Videokamera mit dem Verweis auf entsprechende gewerberechtliche und zivilrechtliche Verfahren, für welche sie Beweismittel sicherstellen müsse.

In der vorliegenden Sache erfolgte eine permanente Beweissicherung durch Bildaufnahmen u.a. zwecks Erstattung von Verwaltungsstrafanzeigen bzw. zur Gewinnung von Beweismitteln für ein zivilrechtliches Verfahren. Zwar hatte die Datenschutzbehörde es nach ihrer Rechtsprechung für zulässig erachtet, anlassbezogen verarbeitete Bilddaten im vertretbaren Ausmaß an eine zuständige Verwaltungsstrafbehörde für den Zweck der Erstattung einer Anzeige zu übermitteln, im konkreten Fall handelte es sich jedoch nicht um eine anlassbezogene Bilddatenverarbeitung, sondern ging die Datenschutzbehörde von einer regelmäßigen Überwachung der betroffenen Liegenschaft des Einschreiters aus. Diese Art der Beweismittelgewinnung – nämlich durch eine Videoüberwachung – war für unzulässig zu erachten und daher sprach die Datenschutzbehörde eine entsprechende Empfehlung aus, dass die Antragsgegnerin die mittels Videoüberwachung durchgeführte Ermittlung, Speicherung und Übermittlung von personenbezogenen Daten (etwa auf dem Grundstück des Einschreiters beschäftigte oder wohnhafte Personen sowie Kennzeichen von Kraftfahrzeugen) durch Fotos, Video- oder Audiosequenzen zum Zwecke des Beweises von behaupteten Verwaltungsübertretungen bzw. zur Geltendmachung zivilrechtlicher Ansprüche unterlassen möge.

3.2.3 Rechtsauskünfte an Bürgerinnen und Bürger

Die Datenschutzbehörde stellt auf ihrer Website unter https://www.dsb.gv.at/fragen-und-antworten umfassende Informationen im Zusammenhang mit dem Datenschutzrecht zur Verfügung. Diese Informationen umfassen leicht verständliche Antworten auf die relevantesten datenschutzrechtlichen Fragen. Darüber hinaus finden sich auf der unter https://www.dsb.gv.at/rechte-der-betroffenen ausführliche Informationen über die Rechte der Betroffenen und die Verfahrensarten nach dem DSG 2000. Zu beachten ist, dass die Datenschutzbehörde ihre Website im Hinblick auf die Datenschutz-Grundverordnung (DSG-VO), die ab 25. Mai 2018 Anwendung findet, inhaltlich anpassen wird. Bereits jetzt darf auf den Leitfaden zur DSG-VO hingewiesen werden, der unter https://www.dsb.gv.at/dokumente zum Download verfügbar ist.

Darüber hinaus beantwortet die Datenschutzbehörde auch weiterhin allgemeine Anfragen zum Datenschutz schriftlich. Telefonische Rechtsauskünfte werden nicht erteilt. Die Datenschutzbehörde nimmt im Rahmen einer Rechtsauskunft keine auf den Einzelfall bezogene inhaltliche rechtliche Beurteilung vor. Diese rechtlichen Beurteilungen können auf Grund der gesetzlichen Zuständigkeit der Datenschutzbehörde nur im Zuge eines konkreten Verfahrens vorgenommen werden. Jede Vorabbeurteilung würde das Ergebnis eines allfälligen Verfahrens vor der Datenschutzbehörde vorwegnehmen.

3.2.4 Genehmigungen im Internationalen Datenverkehr

Die Anzahl der Anträge für Genehmigungen im Internationalen Datenverkehr ist im Verhältnis zu 2016 im Jahr 2017 auf 185 zurückgegangen. Diese Zahl ist immer noch deutlich höher als in den Jahren 2014 und 2015.

Die im Jahr 2016 eingeführte Vorgangsweise, nicht-juristische Sachbearbeiter in die Bearbeitung der Anträge einzubinden, hat sich bewährt.

Mit dem neuen Rechtsrahmen der Datenschutz-Grundverordnung werden ab Mai 2018 fast alle bisher genehmigungspflichtigen Fälle von internationalem Datenverkehr genehmigungsfrei. Dies betrifft die Weitergabe von Daten mit den bisher gebräuchlichsten Instrumenten, Standardvertragsklauseln (Art. 46 Abs. 1 lit. c und d DSGVO) und Binding Corporate Rules (Art. 46 Abs. 1 lit. b, 47 DSGVO).

Die im Jahr 2016 mit dem Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes geschaffene Rechtsgrundlage für den genehmigungsfreien Datenverkehr mit den USA („EU-U.S. Privacy Shield"), zeigte ihre Wirkung. Es waren weniger Anträge auf Datenweitergabe in die USA zu genehmigen. Es zeigte sich – wie im Vorjahr – dass die Privilegierung des EU-U.S. Privacy Shields noch immer nicht ausreichend genutzt wird. Mehrere Unternehmen, die Anträge zur Genehmigung im internationalen Datenverkehr eingebracht hatten, mussten von der Behörde informiert werden, dass für diese Weitergabe Genehmigungsfreiheit besteht.

Es ist zu erwarten, dass die Datenschutz-Grundverordnung (DSG-VO) im Jahr 2018 einen drastischen Rückgang der Anträge auf Genehmigung im Internationalen Datenverkehr bewirken wird.

3.2.5 Entscheidungen im Registrierungsverfahren

Registrierungen:

a. Registriert wurden von der ASFINAG gemeldete Datenanwendungen im Zusammenhang mit der Einführung der „Digitalen Vignette". Hierbei handelt es sich um ein System zur Entrichtung, Verwaltung und Kontrolle der zeitabhängigen Maut für mautpflichtige Kraftfahrzeuge auf mautpflichtigen Autobahnen und Schnellstraßen. Die digitale Vignette ist als elektronische Alternative zur Klebevignette konzipiert. Erforderlich ist die einmalige Registrierung des KFZ-Kennzeichens im Mautsystem. Die Kontrolle erfolgt vollautomatisch durch das Aufnehmen von Bilddaten des Fahrzeuges und dem Abgleich mit einer Liste derjenigen KFZs, für welche die Maut elektronisch entrichtet wurde. Bilddaten und daraus gewonnene Kennzeichen- und Kontrolldaten, die Fälle ordnungsgemäßer Entrichtung der Maut betreffen, werden unverzüglich in nicht rückführbarer Weise gelöscht. Bilddaten, die Fälle der Mautprellerei dokumentieren, dürfen im Mautsystem gespeichert, aber nur für Zwecke der Einbringung der Maut, der Aufforderung zur Zahlung einer Ersatzmaut und der Verfolgung von Mautprellerei verwendet werden. Unter anderem bilden die §§ 16a und 19a Bundesstraßen-Mautgesetz 2002 die entsprechenden Rechtsgrundlagen für die Datenverwendung.

b. Registriert wurde die von der Landespolizeidirektion Niederösterreich gemeldete Datenanwendung „Automatisierte Grenzkontrolle - eGates (Automated Bordercontrol -eGates)". Zweck der Datenverarbeitung ist die Durchführung einer automationsunterstützten Grenzkontrolle durch den Einsatz elektronischer Abfertigungsgeräte. Dazu werden die im Zusammenhang mit der Grenzkontrolle automatisationsunterstützt ermittelten personenbezogenen Daten (darunter auch Bilddaten der Betroffenen) für die Dauer des elektronischen Ab-

fertigungsprozesses verarbeitet und für Fahndungsabfragen im Rahmen der Sicherheitsverwaltung und der Tätigkeit der Sicherheitsbehörden im Dienste der Strafrechtspflege verwendet. Rechtsgrundlagen sind der Schengener Grenzkodex und das Grenzkontrollgesetz.

c. Nachdem 2016 die anlassbezogene Videoüberwachung („BodyCams")" im Bereich öffentlicher ÖBB-Verkehrsstationen registriert wurde, wurde 2017 auch die Datenanwendung „Anlassbezogener Einsatz einer Videoüberwachung zur Dokumentation sicherheitskritischer Situationen („BodyCams") durch Mitarbeiter im Zugbegleitdienst der Ostregion der ÖBB-Personenverkehr AG registriert. Der Einsatz dieser Bodycams dient folgenden Zwecken; 1. Gewährleistung der Sicherheit und Ordnung des Zugbetriebes; 2. Objektschutz (Schutz der Personenzüge samt der Zugeinrichtungen); 3. Schutz von Personen (insbesondere von Kunden und Mitarbeitern der ÖBB-Personenverkehr AG); 4. Verhinderung und Eindämmung straf- und zivilrechtlich relevanten Verhaltens (Generalprävention); 5. Beweissicherung im Anlassfall (dh bei einer Gefährdung, Verletzung oder Beschädigung von Personen oder Objekten zur Aufklärung von straf- und zivilrechtlich relevanten Verhaltens); 6. Gerichtliche und versicherungsrechtliche Abwicklung von Anlassfällen; 7. Beweisgrundlage für die interne Vorfallsuntersuchung der ÖBB-Personenverkehr AG sowie 8. Grundlagenmaterial für interne Schulungen. Die so aufgenommenen Videoaufzeichnungen werden im Regelfall 72 Stunden verschlüsselt gespeichert. Eine Datenübermittlung erfolgt nur im gerechtfertigten Anlassfall.

Ablehnungen:

a. Abgelehnt wurde die durch einen Forstbetrieb gemeldete Videoüberwachung in dessen Waldgebiet (unter anderem auch im Bereich der Ein- und Ausfahrten). Dabei war geplant die Videoüberwachung auch zum Zweck der Kontrolle von Belade- und Transportvorgängen im Zusammenhang mit Holzlieferungen einzusetzen. Gemäß § 50a Abs. 2 DSG 2000 sind rechtmäßige Zwecke einer Videoüberwachung, insbesondere die Auswertung und Übermittlung der dabei ermittelten Daten, jedoch nur der Schutz des überwachten Objekts oder der Schutz der überwachten Person oder die Erfüllung rechtlicher Sorgfaltspflichten. Die Kontrolle von Beladevorgängen und des nachfolgenden Abtransports durch Mitarbeiter Dritter (Frächter) mittels einer Videoüberwachung stellte - unabhängig davon, ob eine diesbezügliche Einwilligung der Betroffenen vorliegt oder nicht - nach Ansicht der Datenschutzbehörde keinen rechtmäßigen Zweck im Sinne des § 50a Abs. 2 DSG 2000 dar und wurde somit im konkreten Fall als unzulässig angesehen.

b. Abgelehnt wurde die durch einen Verein gemeldete Datenanwendung automatische fotografische Überwachung von LKW im Bereich von Autobahnab- und auffahrten, welche in das Salzkammergut einfahren und aus dem Salzkammergut ausfahren". Die Bilddatenaufzeichnung sollte dazu dienen, der Bezirksverwaltungsbehörde Beweismaterial im Zusammenhang mit der Verletzung verkehrsrechtlicher Bestimmungen zu liefern. Die Datenschutzbehörde vertrat in diesem Verfahren die Ansicht, dass dem Verein die erforderliche „gesetzliche Zuständigkeit" bzw. „rechtliche Befugnis" im Sinne des § 7 Abs. 1 DSG 2000 zur Überwachung öffentlicher Straßen wie insbesondere von Autobahnab- und auffahrten fehlt.

c. Abgelehnt wurden im Berichtszeitraum drei Meldungen von Hinweisgebersystemen, welche durch politische Parteien bzw. einen Parlamentsclub eingebracht wurden. Im Rahmen dieser Systeme sollten Bürger dazu aufgefordert werden, Missstände unterschiedlicher Art (auch Verbrechen) über das Internet zu melden. In allen Fällen wurde die Registrierung nach einem Verfahren gemäß § 20 Abs. 5 DSG 2000 abgelehnt. Die Datenschutzbehörde vertrat die Meinung, dass politische Parteien oder Parlamentsclubs nicht über die in § 6 und 7 DSG 2000 geforderten gesetzlichen Zuständigkeiten und rechtlichen Befugnisse für eine solche Datenverwendung verfügen. In einem Fall wurde beantragt, über die Ablehnung mittels Bescheid

abzusprechen. Der Bescheid wurde erlassen und im Jänner 2018 eine Beschwerde an das Bundesverwaltungsgericht erhoben. Das diesbezügliche Verfahren ist anhängig.

3.2.6 Stammzahlenregisterbehörde

Allgemeines

Hinter den elektronischen Serviceleistungen der öffentlichen Einrichtungen, die mit der E-ID (früher: Bürgerkarte) oder der Handysignatur sicher genutzt werden können, sind von der Datenschutzbehörde betriebene Datenanwendungen. Ein datenschutzfreundliches System zur eindeutigen Identifizierung von Personen (das Stammzahlenregister), ein Personenregister für Personen, die nicht im zentralen Melderegister einzutragen sind (das Ergänzungsregister für natürliche Personen), das Unternehmensregister in dem alle Unternehmen erfasst werden können, die nicht im Firmenbuch oder Vereinsregister einzutragen sind (das Ergänzungsregister für sonstige Betroffene) und ein Register das vertretungsweises Handeln mittels E-ID oder Handysignatur ermöglicht (das Vollmachtenregister).

Zahlen und Überblick

Stammzahlenregister

Im Jahr 2017 wurden über 264 Millionen bereichsspezifische Personenkennzeichen (bPK) berechnet. Das entspricht einer Steigerung von über 30% im Verhältnis zum Jahr davor. Verantwortlich dafür sind vor allem die Erstausstattungen der Spendenorganisationen. Spenden werden von den Spendenorganisationen seit 2017 verpflichtend direkt an die Finanzbehörden gemeldet und erstmals automatisch in der Arbeiternehmer/innen Veranlagung für das Jahr 2017 übernommen. Die damit verbundenen Umsetzungsmaßnahmen haben sowohl bei der Datenschutzbehörde als auch beim Bundesministerium für Inneres in seiner Funktion als Dienstleister der Datenschutzbehörde zu einer erheblichen Zusatzbelastung geführt.

Vollmachtenregister

2017 wurden 712 neue Vollmachten von der DSB eingetragen. In Vertretung gehandelt wurde 23.733 Mal. Berufsmäßige Parteienvertreter haben das Service 3.436 Mal benutzt.

Die meisten Vertretungsbefugnisse werden automatisch aus dem Firmenbuch, Vereinsregister und Ergänzungsregister für sonstige Betroffene übernommen.

Am häufigsten eingesetzt werden die Vollmachten für Zustelldienste und DVR online.

Ergänzungsregister für natürliche Personen

2017 wurden 106. 377 Transaktionen im Ergänzungsregister für natürliche Personen (Neuanlagen, Änderungen, Beendigungen) durchgeführt. 55.057 davon waren Eintragungen neuer Personen in das Register. Insgesamt waren zum Stichtag 31.12.2016 237.333 Personen eingetragen. Das entspricht einer Steigerung von über 30% im Verhältnis zum Jahr davor.

Ergänzungsregister für sonstige Betroffene

Am Ende des Jahres 2017 enthielt das Register 1.498.301 aktive und 388.831 inaktive Unternehmen. 119.637 Neueintragungen und 1.006.731 Änderungen wurden vorgenommen. Das Register wurde 1.272.280 Mal über die Weboberfläche abgefragt (das entspricht einer Steigerung von über 350% im Vergleich zum Vorjahr) und 31.651.637 Mal von Behörden über die zur Verfügung gestellte Schnittstelle durchsucht.

Die Aufgaben und Datenanwendungen der Stammzahlenregisterbehörde

Erzeugung von bereichsspezifischen Personenkennzeichen

Im E-Government-System erfolgt die eindeutige Identifikation natürlicher Personen durch eine geheime Stammzahl und davon abgeleiteten bereichsspezifischen Personenkennzeichen (bPK). Die Stammzahl wird aus der im zentralen Melderegister verwendeten ZMR-Zahl mit Hilfe eines geheimen Schlüssels gebildet. Der geheime Schlüssel und alle damit verknüpften Funktionen werden von der DSB in ihrer Funktion als Stammzahlenregisterbehörde verwaltet. Die Stammzahl darf bis zum Inkrafttreten der E-Governmentgesetz-Novelle BGBl. I Nr. 121/2017 nur in der E-ID gespeichert werden. Nach Inkrafttreten dieser Novelle darf sie nur mehr von der Stammzahlenregisterbehörde zur Errechnung von bPK verwendet werden.

Die Stammzahlenregisterbehörde erzeugt bPK und stellt sicher, dass diese richtig eingesetzt werden. Zu diesem Zweck müssen Auftraggeber des öffentlichen Bereichs einen Antrag bei der Stammzahlenregisterbehörde auf Erlaubnis der Verwendung oder Ausstattung einer Datenanwendung mit bPK stellen. Ein bereichsspezifisches Personenkennzeichen kann weder auf die Stammzahl zurückgerechnet werden, noch – ohne zusätzliche Angaben über die Person und der Mitwirkung der Stammzahlenregisterbehörde – in ein bereichsspezifisches Personenkennzeichen eines anderen Bereichs umgerechnet werden.

Das erleichtert der öffentlichen Verwaltung die Zuordnung von Personen zu Verfahren, erlaubt es den betroffenen Bürgern mit einem einzigen sicheren Mechanismus öffentliche Dienstleistungen bequem elektronisch abzuwickeln und schützt gleichzeitig die Betroffenen vor einer leichteren Zusammenführbarkeit ihrer Daten. Sichergestellt wird insbesondere, dass es durch die eindeutige elektronische Identifizierung zu keiner einfachen Zusammenführbarkeit der mit bPK verknüpften Daten kommen kann, indem die bPK für verschiedene Bereiche der öffentlichen Verwaltung anders gebildet werden. Dadurch sind diese Kennzeichen in Datenanwendungen eines anderen Bereichs unbrauchbar.

Ergänzungsregister

Die DSB betreibt zwei „Ergänzungs“register, in die sich jene natürlichen Personen und sonstige rechtlich erhebliche Entitäten eintragen lassen können, die in keinem der Basisregister des E-Government-Systems (Zentrales Melderegister, Firmenbuch und Vereinsregister) eingetragen sind.

In das Ergänzungsregister für natürliche Personen (ERnP) können Personen eingetragen werden, die nicht im zentralen Melderegister eingetragen werden müssen.

In das Ergänzungsregister für sonstige Betroffene (ERsB) kann jedes Unternehmen eingetragen werden, das nicht im Firmenbuch oder Vereinsregister erfasst werden muss (z.B. Behörden, Religionsgemeinschaften oder Arbeitsgemeinschaften). Unternehmen und juristische Personen werden im österreichischen E-Government mit bereichsübergreifenden Kennzeichen, die zum Teil auch offen (Firmenbuchnummer) geführt werden, identifiziert. Diese Kennzeichen werden im E-Government Anwendungen als Stammzahl verwendet. Das Ergänzungsregister für sonstige Betroffene schließt die Lücke für jene Unternehmen, die in Österreich kein Kennzeichen haben.

Vollmachtenregister

Das Vollmachtenregister erlaubt vertretungsweises Handeln in E-Government Anwendungen von Personen, deren Einzelvertretungsbefugnis in einem Basisregister des E-Government-Systems (Firmenbuch, Ergänzungsregister für sonstige Betroffene oder Vereinsregister) eingetragen wurde oder durch Ausstellung einer Vollmacht mittels E-ID oder Handysignatur und

Übertragung auf die E-ID oder Handysignatur einer anderen Person. In diesem Zusammenhang weist die DSB auf das vom Bundesministerium für Finanzen betriebene Unternehmensserviceportal (USP) hin, das Unternehmen eine ähnliche Funktionalität anbietet.

Entwicklungen

a. Legistische Entwicklungen – Novellierungen des EGovG

Zwei E-Government Gesetz Novellen haben im Jahr 2017 wesentliche strukturelle Veränderungen des österreichischen E-Government-Systems bewirkt.

Mit der Novelle BGBl. I Nr. 40/2017 wurde im Wesentlichen das Recht auf elektronischen Verkehr für Bürger eingeführt und die Pflicht zur Teilnahme an der elektronischen Zustellung für Unternehmen eingeführt, sowie die Errechnung von bPK ohne Mitwirkung der Betroffenen auf den privaten Bereich ausgedehnt.

Für die Stammzahlenregisterbehörde ergibt sich durch die Umsetzung der Pflicht zur Teilnahme an der elektronischen Zustellung ein progressiv ansteigendes Volumen an Vollmachtenregister-Transaktionen. Diese werden aber wieder zurückgehen, sobald im Unternehmensserviceportal (USP) ein neuer Service zur Berechtigung von Zustellbevollmächtigten die Verwendung des Vollmachtenregisters für die Teilnahme an Zustellservices überflüssig macht. Damit soll auch das aktuelle Teilnahmehindernis von Unternehmen, die keine einzelvertretungsbefugten Personen in den Basisregistern des E-Government-Systems eingetragen haben, gelöst werden.

Die bPK Errechnung ohne Mitwirkung des Betroffenen, die bisher öffentlichen Einrichtungen vorbehalten war, wurde auf den privaten Bereich ausgedehnt. Durch die Umsetzung dieser Novelle ergibt sich sowohl technisch als auch organisatorisch eine potentiell große Herausforderung für die Datenschutzbehörde, da sich der bisher auf (österreichische) öffentliche Einrichtungen beschränkte Beratungs-, Prüf- und Umsetzungsaufwand durch diese Novelle auf theoretisch jedermann ausdehnt.

Mit der Novelle BGBl. I Nr. 121/2017 wurde im Wesentlichen die EIDAS Verordnung [1] umgesetzt und einige Eckpfeiler des E-Government-Systems. Die zwei wichtigsten Änderungen sind der erhöhte Schutz der Stammzahl und die Registrierung der E-ID durch die Passbehörden.

Die Funktion E-ID wird in Zukunft nur mehr das bPK verwenden. Die bisher vorübergehend zur lokalen Berechnung von bPK bereitgestellte Stammzahl wird in Hinkunft nur mehr bei der Stammzahlenregisterbehörde kurzfristig (z.B. im Zuge einer bPK Erzeugung) berechnet oder verwendet. Sie darf darüber hinaus nur von einem von ihr beauftragten Vertrauensdiensteanbieter in verschlüsselter Form für die Berechnung von bPK durch die Stammzahlenregisterbehörde dauerhaft gespeichert werden.

In Zukunft werden E-ID und Handysignatur von den Passbehörden (oder ähnlichen gleichwertigen Behörden) aktiviert. Damit wird der bereits sehr hohe Qualitätsstandard bei der eindeutigen Identifizierung der Teilnehmer nochmals gehoben, insbesondere, weil dadurch langfristig sichergestellt werden kann, dass elektronische Identitäten und Ausweisdaten nicht mehr voneinander abweichen können.

1 Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

b. Operative Entwicklungen

b.1 „Spendenpaket“
Im Jahr 2017 wurden vom Bundesministerium für Finanzen zahlreiche Informationsveranstaltungen für Spendenorganisationen betreffend der Umsetzung des „Spendenpakets“ abgehalten, es erfolgte die produktive Inbetriebnahme des sognannten File-Upload Verfahrens mit August 2017, eine von mehreren möglichen technischen Varianten zur Umsetzung des Spendenpakets. Zur Erinnerung: Durch die Einfügung eines Absatzes 8 zu § 18 Einkommensteuergesetz 1988 im Rahmen des Steuerreformpakets 2015/16“[2] wurde festgelegt, dass z.B. Spenden, Beiträge im Rahmen der Weiterversicherung in der gesetzlichen Pensionsversicherung oder der Kirchenbeitrag nur dann als Sonderausgaben zu berücksichtigen sind, wenn dem Empfänger (beispielsweise der Spendenorgansiation) Vor- und Zunamen und das Geburtsdatum des Leistenden bekannt gegeben werden und eine Datenübermittlung mittels vBPK-SA an die Finanz erfolgt.

Eine weitere technische Variante - das sogenannte Dialogverfahren (bei dem die Spendenorganisation die Daten der Spender direkt in eine vorgegebene Eingabe-Maske in FinanzOnline eingeben), geht mit Anfang des Jahres 2018 in Betrieb.

Bis Ende 2017 wählten mehr als 360 Spendenorganisationen den File-Upload als technische Zugangsvariante. Mehr als 120 Spendenorganisationen waren über eine Online Schnittstelle angebunden.

Weitere Informationen sind unter folgenden Links zu finden:
https://www.bmf.gv.at/steuern/selbststaendige-unternehmer/einkommensteuer/FAQ-automatische-Datenuebermittlung-SA.html#heading_16__Was_passiert__wenn_die_Datenuebermittlung_nicht_rechtzeitig__bis_Ende_Februar_des_Folgejahres__erfolgt_

https://www.bmf.gv.at/steuern/selbststaendige-unternehmer/einkommensteuer/Praesentation_Datenuebermittlung_Sonderausgaben_fuer_Uebermi.pdf?67ry6u

b.2 „Wirtschaftliches Eigentümer-Register“
Mit 15.9.2017 wurde im BGBl. I Nr. 136/2017 das Wirtschaftliche Eigentümer Registergesetz kundgemacht. Demnach wird zum Zwecke der Verhinderung von Geldwäscherei und Terrorismusfinanzierung beim Bundesministerium für Finanzen als Registerbehörde ein Register der wirtschaftlichen Eigentümer eingerichtet. Gemäß § 2 des neuen WiEReG sind wirtschaftliche Eigentümer alle natürlichen Personen, in deren Eigentum oder unter deren Kontrolle ein Rechtsträger letztlich steht.

Die „einmeldeverpflichteten“ Rechtsträger sind in § 1 Abs. 2 WiEReG aufgezählt. Die Rechtsträger sind gemäß § 3 WiEReG verpflichtet, ihre wirtschaftlichen Eigentümer festzustellen, zu überprüfen und im elektronischen Wege über das Unternehmensserviceportal des Bundes zu melden. Seit dem Inkrafttreten am 15. Jänner 2018, können Meldungen über das Unternehmensserviceportal des Bundes an das Register übermittelt werden.

Zum Zwecke der eindeutigen Identifikation von wirtschaftlichen Eigentümern wird über das Stammzahlenregister automatisationsunterstützt das bereichsspezifische Personenkennzeichen des Bereichs „Steuern und Abgaben – SA“ ermittelt.

2 https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2015_I_118/BGBLA_2015_I_118.pdf

Mit BGBl. I Nr. 150/2017 vom 10. November 2017 wurde zusätzlich eine Abfragemöglichkeit im Ergänzungsregister für natürliche Personen geschaffen.

Weiter Informationen unter folgendem Link:
https://www.bmf.gv.at/finanzmarkt/register-wirtschaftlicher-eigentuemer/Karussell/das-register.html

b.3 „E-ID Konzept, EiDAS Umsetzung"
Die Stammzahlenregisterbehörde nahm an zahlreichen interministeriellen Besprechungen zur Umsetzung des E-ID Architekturkonzeptes teil. Eine Notifizierung im Sinne von Art. 9 der eIDAS Verordnung (910/2014/EU) an die Europäische Kommission ist bis 31.1.2018 nicht erfolgt.

3.2.7 Amtswegige Prüfverfahren

Die DSB hat im Jahr 2017 93 amtswegige Verfahren nach § 30 DSG 2000 eingeleitet; 106 amtswegige Verfahren wurden im Berichtszeitraum abgeschlossen.

Ausgewählte Verfahren
Neben den amtswegigen Verfahren, die aufgrund anonymer Eingaben oder Eingaben durch Behörden erfolgen (überwiegend zur Überprüfung der Rechtmäßigkeit einer Videoüberwachung), führt die Datenschutzbehörde seit 2014 jährlich Schwerpunktverfahren durch.

Dabei wird ein bestimmter Sektor einer eingehenden datenschutzrechtlichen Überprüfung – einschließlich Vorortuntersuchungen – unterzogen.

2014/2015 wurden die wesentlichen Kreditauskunfteien näher geprüft. In den Jahren 2015/2016 wurden die größten Krankenanstaltenträger in allen neun Bundesländern einer Prüfung unterzogen. Im Berichtsjahr wurden einige Versicherungsunternehmen in den Bereichen der Kranken-, Unfall- und Lebensversicherungen geprüft.

Wenn nicht anderes angeführt ist, sind sämtliche Entscheidungen im Rechtsinformationssystem des Bundes (RIS) abrufbar.

D213.468 bis D213.471
Diese Verfahren dienten der Fortsetzung der Umsetzung des Prüfungsschwerpunktes 2015/2016 im Krankenanstaltenbereich. Die Datenschutzbehörde prüfte dabei jene öffentlichen Krankenanstaltenträger in vier Bundesländern, die 2015 noch keiner Überprüfung unterzogen wurden. Diese Verfahren wurden 2016 begonnen und im Berichtszeitraum mit Empfehlungen abgeschlossen.

D213.475
Dieses Verfahren betrifft die Verwendung von Gesundheitsdaten in militärischen Sanitätszentren und war vom Prüfungsschwerpunkt 2015/2016 umfasst. Dieses Verfahren wurde im Berichtszeitraum mit einer Empfehlung abgeschlossen, die Entscheidung ist im RIS nicht abrufbar.

D213.529 bis D213.534
Diese Verfahren dienten der Umsetzung des Prüfungsschwerpunktes 2017 im Versicherungsbereich und wurden im Berichtszeitraum abgeschlossen. Die Datenschutzbehörde prüfte dabei sechs große Versicherungsunternehmen in Österreich, ob in den Sparten der Kranken-, Unfall- und Lebensversicherungen datenschutzrechtliche Bestimmungen eingehalten werden.

Das Prüfverfahren ergab, dass datenschutzrechtliche Bestimmungen im überwiegenden Ausmaß eingehalten werden und dass der Schutz personenbezogener Daten integraler Bestandteil interner Beurteilungen und Verfahrensabläufe ist. Auch konnte festgestellt werden, dass die DSGVO bei der Ausgestaltung von Abläufen bereits Berücksichtigung findet.

Alle Verfahren wurden mit Empfehlungen abgeschlossen.

Die Empfehlungen betreffen im Wesentlichen folgende Punkte:
- mangelnde Löschroutinen bei Kundendaten sowie bei Daten ehemaliger Bediensteter
- mangelhafte Umsetzung von Auflagenbescheiden der Datenschutzbehörde
- mangelhafte oder unterlassene Meldungen im DVR

D213.535 und D213.547
Diese Prüfverfahren betrafen die Datenverwendung zum Zweck der „Pfuscherbekämpfung" durch eine Wirtschaftskammer und durch mehrere Bezirksverwaltungsbehörden. Die Verfahren wurden im Berichtszeitraum mit Empfehlungen abgeschlossen.

D213.542
Dieses Prüfverfahren betraf die Überprüfung der nationalen Komponente des Schengener Informationssystems (N.SIS). Die Datenschutzbehörde ist aufgrund europarechtlicher Vorgaben verpflichtet, das N.SIS in periodischen Abständen zu prüfen. Diese Prüfung wurde, auch weil sie die technische Komponente des N.SIS miteinbezog, unter Beiziehung zweier nicht-amtlicher technischer Sachverständiger durchgeführt.

Das Verfahren wurde mit einer Empfehlung abgeschlossen, die zum Zeitpunkt der Berichtslegung noch nicht im RIS verfügbar ist.

3.2.8 Äußerungen in Beschwerdeverfahren vor dem Bundesverwaltungsgericht

Die Anzahl der Beschwerden an das Bundesverwaltungsgericht hat sich gegenüber dem Vorjahr nur wenig geändert.

Im Berichtszeitraum wurde keine Beschwerde wegen Verletzung der Entscheidungspflicht eingebracht.

Entscheidung W101 2016270-1 vom 4. April 2017
Das Bundesverwaltungsgericht behandelte eine Beschwerde gegen einen Bescheid der Datenschutzbehörde, mit dem die Meldung einer Dashcam beim Datenverarbeitungsregister abgelehnt wurde. Eine „Dashcam" ist eine am Auto angebrachte Videokamera, die das Verkehrsgeschehen aufnimmt.

Das Bundesverwaltungsgericht entschied gegen den Auftraggeber, aber mit einer anderen Begründung als die Datenschutzbehörde. Die Datenschutzbehörde hatte die Meldung der Dashcam mit der Begründung abgelehnt, dass er für die Überwachung des öffentlichen Raumes keine „gesetzliche Zuständigkeit" bzw. „rechtliche Befugnis" iSd § 7 Abs. 1 DSG 2000 vorweisen konnte.

Das Bundesverwaltungsgericht entschied, dass eine rechtliche Befugnis eines privaten Auftraggebers zum Betrieb einer Videoüberwachungsanlage, die auch auf öffentlichen Raum gerichtet ist, nicht grundsätzlich verneint werden kann. Das Bundesverwaltungsgericht hob aber den Bescheid nicht auf, weil der Eingriff durch die Dashcam offenkundig unverhältnismäßig war.

Die gemeldete Videoüberwachung war jedenfalls nicht das gelindeste Mittel iSd § 7 Abs. 3 DSG 2000. Im Ergebnis gab es daher keinen Unterschied.

Entscheidung W214 2117640-1 vom 11. Juli 2017
Ein Auftraggeber hatte für eine erteilte Auskunft eine Gebühr in Höhe von insgesamt 20,78 Euro in Rechnung gestellt, die auch von der Beschwerdeführerin beglichen wurde. Die Beschwerdeführerin forderte das Geld in einer Beschwerde zurück.

Die Datenschutzbehörde hatte die Beschwerde in diesem Punkt zurückgewiesen, das Bundesverwaltungsgericht bestätigte diese Entscheidung. Bei der Gebühr handelt es sich nicht um Verfahrenskosten im Sinne des § 74 AVG. Sollte der Auftraggeber Kosten rechtswidrig auf die Beschwerdeführerin übergewälzt und damit ihr Vermögen gemindert haben, liegt auf Seiten der Beschwerdeführerin ein Schadenersatz- oder Bereicherungsanspruch gegen den Auftraggeber vor.

Entscheidung W101 2113680-1 vom 29. September 2017
Im Berichtszeitraum wurde auch eine Entscheidung der Datenschutzbehörde als Stammzahlenregisterbehörde vor das Bundesverwaltungsgericht gebracht. Ein Elternpaar hatte die Ausstellung einer Bürgerkarte für die minderjährige Tochter beantragt. Weiters wurde die Eintragung der Vertretungsbefugnis der Eltern des minderjährigen Kindes in deren Bürgerkarten beantragt.

Die Datenschutzbehörde wies den Antrag auf Ausstellung einer Bürgerkarte zurück, weil kein geeignetes Signaturprodukt vorgelegt worden war auf dem die erforderliche Personenbindung eingetragen werden konnte. Der Antrag auf Eintragung einer Vertretungsbefugnis wurde abgewiesen, weil die in § 9 Abs. 2 Stammzahlenregisterbehördenverordnung 2009 (StZRegBehV 2009) vorgesehenen Nachweise nicht erbracht werden konnten. Als Nachweis geeignet sind: eine Bestätigung der Vertretungsbefugnis durch den Vertretenen oder die Vorlage geeigneter Urkunden, wenn glaubhaft gemacht werden kann, dass der Vertretene von der Eintragung Kenntnis hat. Weil Daten über die Vertretungsbefugnis einer Person immer auf dem neuesten Stand gehalten werden müssen, kann eine solche Eintragung in der Regel nur bei Nachweis einer Eintragung über eine Einzelvertretungsbefugnis in einem öffentlichen Register erfolgen.

Das Bundesverwaltungsgericht änderte die Entscheidung der Datenschutzbehörde ab. Die Beschwerde wurde mangels Geschäftsfähigkeit der Antragstellerin als unzulässig zurückgewiesen. Eine Revision beim Verwaltungsgerichtshof ist anhängig.

3.2.9 Stellungnahmen zu Gesetzes- und Verordungsentwürfen

Die DSB hat im Jahr 2017 zu folgenden Vorhaben eine Stellungnahme abgegeben. Die Stellungnahmen sind, soweit es sich nicht jene zu Verordnungen oder Landesgesetzen handelt, unter www.parlament.gv.at abrufbar.

- Entwurf eines Bundesgesetzes, mit dem das Gesundheitsberuferegister-Gesetz, das Gesundheits- und Krankenpflegegesetz und das MTD-Gesetz geändert werden (GBRG-Novelle 2017)
- „kleine Ökostromnovelle“
- Novelle zum Polizeikooperationsgesetz
- Arbeitsmarktintegrationsgesetz
- Integrationsgesetz
- Änderung der Meldegesetz-Durchführungsverordnung
- Bundesgesetz, mit dem das Insolvenz-Entgeltsicherungsgesetz geändert wird
- Sozialversicherungs-Zuordnungsgesetz

- Gesetzespaket zur MiFID II-Umsetzung
- Bundesgesetz, mit dem das Bilanzbuchhaltungsgesetz 2014 geändert wird
- Wirtschaftstreuhandberufsgesetz 2017
- Bundes-Sportförderungsgesetz 2017 u.a.
- Novelle der Kommunikations-Erhebungs-Verordnung
- Wirtschaftliche Eigentümer Registergesetz
- Änderung des Suchtmittelgesetzes
- Änderung der Suchtgiftverordnung
- Datenschutz-Anpassungsgesetz 2018
- Privatstiftungsgesetz- Novelle 2017
- Strafprozessrechtsänderungsgesetz 2017
- Versicherungsvertriebsgesetz 2017
- Änderung des SPG, BStMG 2002, StVO, TKG 2003
- Änderung der Intelligenten Messgeräte-Einführungs-VO
- Zahlungsdienstegesetz 2018 (PSD II Umsetzung)
- Wiener Datenschutz-Anpassungsgesetz

4 Wesentliche höchstgerichtliche Entscheidungen

4.1 Verfahren vor dem Verfassungsgerichtshof

Im Berichtszeitraum hat sich der Verfassungsgerichtshof (VfGH) mit folgenden, für das Datenschutzrecht und das Verfahren von der DSB relevanten, Fällen befasst:

Im Beschluss vom 22.02.2017, G 426/2016 hat der VfGH einen Verfahrenshilfeantrag zwecks Stellung eines Individualantrags auf Prüfung der Verfassungsmäßigkeit des § 3 Abs. 5 des Wählerevidenzgesetzes 1973 (WEvG) wegen Aussichtslosigkeit abgewiesen. Begründet wurde dies mit der Möglichkeit, gegen die dort vorgesehene Datenübermittlung an die zur Außenvertretung berufenen Organe der im Nationalrat vertretenen Parteien gemäß § 31 Abs. 2 DSG 2000 eine Beschwerde an die Datenschutzbehörde zu richten. Dieser Rechtsschutzweg sei zumutbar.

Im Gefolge dieser Beschwerde ist keine entsprechende Beschwerde bei der DSB eingelangt. § 3 Abs. 5 WEvG ist mit 1. Jänner 2018 außer Kraft getreten und durch Bestimmungen des Wählerevidenzgesetzes 2018 (§ 4 Abs. 2) ersetzt worden.

Im Erkenntnis vom 29. November 2017, G223/2016 hatte der VfGH einen sogenannten „Drittelantrag“ von Abgeordneten des Nationalrats betreffend die Verfassungsmäßigkeit des Polizeilichen Staatsschutzgesetzes (PStSG) zu prüfen. Der Antrag wurde teils ab-, teils zurückgewiesen.

In datenschutzrechtlicher Hinsicht hat sich der VfGH dabei vor allem mit Bedenken gegen die Ermittlungsermächtigungen gemäß §§ 10 und 11 PStSG befasst. Der VfGH kam dabei zu dem Schluss, dass sich durch § 11 Abs. 1 Z 7 PStSG Möglichkeiten eröffnen, Verkehrsdaten in einer Weise und über einen Zeitraum so zu verknüpfen, dass im Ergebnis Inhalte der Kommunikation (ermittlungstechnisch) vermutet werden können. Dennoch seien diese Daten (Telefonnummern, statische oder dynamische IP-Adressen, Zeitpunkt und Dauer der Kommunikation, die Stammdaten uä) nicht solche, die als eine von Art. 10a StGG geschützte Kommunikation zu qualifizieren sind (vgl VfSlg 19.657/2012). Hingegen greife die Bestimmung des § 11 Abs. 1 Z 7 PStSG in das verfassungsgesetzlich gewährleistete Recht auf Datenschutz gem § 1 Abs. 1 DSG 2000 iVm Art. 8 EMRK ein, verletze dieses jedoch nicht.

Im Erkenntnis vom 12. Dezember 2017, E 3249/2016 hatte sich der VfGH erstmals inhaltlich mit dem von ihm selbst durch interpretatorische Lückenfüllung geschaffenen Recht auf Aktenvernichtung (VfGH, E 10.12.2014, VfSlg 19.937/2014, vgl. Datenschutzbericht 2014, 27) zu befassen. In Fällen, in denen Daten nicht in einer Datenanwendung oder manuellen Datei sondern in Form von eim Verfahren dokumentierendem Verwaltungsakten vorliegen, ist das Grundrechtrecht auf Datenschutz (Löschung von Akteninhalten) bzw. das Recht auf Schutz des Privat- und Familienlebens nicht vor der DSB sondern in dem für das dokumentierte Verfahren geltenden Rechtszug durchzusetzen.

VfGH gab der Beschwerde gegen ein Erkenntnis des Bundesfinanzgerichts (BFG) betreffend einen auf § 1 DSG 2000 und Art. 3 und 8 EMRK gestützten Antrag auf „Löschung“ von Akten eines Finanzamts Folge, und stellte eine Verletzung im Grundrecht nach Art. 8 EMRK in Folge unzutreffender und unzureichender Begründung der Abwägungsentscheidung fest. Das BFG habe es unterlassen, sich mit der Frage näher auseinanderzusetzen, welche Unterlagen betreffend das

Privatleben der Betroffenen tatsächlich zwingend für welche möglichen zukünftigen Verfahren der Abgabenbehörden erforderlich seien. Ausdrücklich hielt der VfGH dabei fest: „Die Möglichkeit eines künftigen Verfahrens beim Europäischen Gerichtshof für Menschenrechte vermag ein Überwiegen des öffentlichen Interesses an der Aufbewahrung der Papierakten gegenüber dem verfassungsgesetzlich gewährleisteten Recht der Beschwerdeführerin auf Achtung ihres Privat- und Familienlebens gemäß Art. 8 EMRK nicht zu begründen." Ähnliche Erwägungen würden für andere vom BFG aufgezählte Verfahren gelten.

Im Jahr 2017 hat der Verfassungsgerichtshof (VfGH) kurz vor Ende des Berichtszeitraums in einer nicht von der DSB ausgehenden und nicht materielles Datenschutzrecht betreffenden Sache eine weitreichende Entscheidung getroffen, die für die künftige Rolle der DSB als Verwaltungsstrafbehörde (Zuständigkeit zur Verhängung von Geldbußen gemäß Art. 83 DSGVO und Verwaltungsstrafen gemäß § 62 DSG) von entscheidender Bedeutung sein könnte.

Unter ausdrücklichem Abgehen von früherer Rechtsprechung hat der VfGH im Erkenntnis vom 13. Dezember 2017, G 408/2016 ua in einem (vom Bundesverwaltungsgericht eingeleiteten Gesetzesprüfungsverfahren), festgehalten, dass die Höhe der angedrohten Sanktion sich „im Ergebnis als kein taugliches Mittel für die Abgrenzung des gerichtlichen Strafrechts und des Verwaltungsstrafrechts" erweist. Der VfGH hält fest, dass diese frühere Rechtsprechung die unterschiedliche Funktion der Geldstrafe im gerichtlichen und im Verwaltungsstrafrecht sowie die mit ihrer Verhängung jeweils einhergehenden Folgen außer Acht lässt. Er verweist zur Begründung weiters auf die Anforderungen, die sich aus dem Unionsrecht ergeben können, sowie auf die inzwischen gegebene Möglichkeit, das Straferkenntnis einer Verwaltungsbehörde durch ein Verwaltungsgericht mit Vollkognition (Prüfbefugnis in jeder Hinsicht, einschließlich der Pflicht, selbst Beweise aufzunehmen, sowohl was Tatsachen als auch was rechtliche Schlussfolgerungen anbelangt) überprüfen zu lassen.

Der VfGH kommt so zu dem Schluss, dass auch die Verhängung sehr hoher Geldstrafen durch eine Verwaltungsbehörde (dort: die Finanzmarktaufsichtsbehörde - FMA), wie sie in § 99d des Bankwesengesetzes (BWG) vorgesehen ist, der Verfassung entspricht.

Diese Entscheidung ist für die Datenschutzbehörde von besonderer Bedeutung, da die Materialien zum Datenschutz-Anpassungsgesetz 2018 die vom VfGH geprüfte Bestimmung des § 99d BWG ausdrücklich als Vorbild für insbesondere § 30 DSG nennen.

4.2 Oberster Gerichtshof

6 Ob 115/17f
Videoüberwachung mit Privatzonenmarkierung auf Eigengrund, wobei der teilweise öffentliche Grund bzw. den Nachbargrund erfassende Bereich durch eine hinterlegte „Privatzone" ausgeblendet (geschwärzt) und daher weder am Überwachungsbildschirm noch in den aufgezeichneten Videodaten dargestellt wird.

Der Oberste Gerichtshof in Zivilrechtssachen hat in seiner Entscheidung 6 Ob 115/17f[3] vom 21.11.2017 im Zuge eines Unterlassungsbegehrens (gerichtet auf eine Videoüberwachung) und

3 https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20171121_OGH0002_0060OB00115_17F0000_000

eines Beseitigungsbegehrens (gerichtet auf die hergestellten Aufzeichnungen) nachfolgende Entscheidungen getroffen (und der Revision der klagenden Partei (Kreditinstitut) nicht Folge gegeben).

Gestützt auf die Feststellungen der Vorinstanzen und einen Sachverständigenbefund, wonach zwar Teile des öffentlichen Grundes und der Liegenschaft der Klägerin (vis à vis Nachbarin) von der Kamera erfasst werden, jedoch durch eine sogenannte Privatzonenmarkierung geschwärzt werden und diese Einstellungen nur durch ein zweiteiliges Passwort der technischen Firma und der Beklagten abänderbar sind, verneinte der OGH die Betroffeneneigenschaft der Klägerin (vis à vis Nachbarin) im Sinne des § 4 Z. 3 DSG 2000.

Mangels Betroffeneneigenschaft verneinte der OGH auch einen Beseitigungsanspruch im Sinne eines Löschungsanspruchs bereits vorhandener Aufzeichnungen.

Hintergrund: Die Klägerin begehrte es zu unterlassen ihre vis à vis gelegene Liegenschaft mit Videokameras zu überwachen und bestehende Aufzeichnungen zu beseitigen. Die Befundaufnahme ergab die erwähnten Privatzonenmarkierungen, deren Einstellungsänderung nur durch ein zweiteiliges Passwort (technische Firma und Beklagte) abänderbar sind. Das Erstgericht wies das Klagebegehren ab, das Berufungsgericht gab der Berufung teilweise Folge und verpflichtete die Beklagte auf Grundlage von § 16 ABGB („Überwachungsdruck“) die das Filmen der Liegenschaft der Klägerin zu unterlassen. Das Beseitigungsbegehren im Sinne einer Löschung von Aufzeichnungen wies das Berufungsgericht ab.

6 Ob 217/16d[4] Präklusionsfrist gemäß § 34 Abs. 1 DSG 2000
Der Oberste Gerichtshof in Zivilrechtssachen hat in seiner Entscheidung 6 Ob 217/16d vom 29.05.2017 im Zuge eines - durch zwei Instanzen stattgegebenen Unterlassungs- und Beseitigungsbegehrens eines KKE Eintrages – nachfolgende Erwägungen zur Auslösung der „Kenntnis eines beschwerenden Ereignisses“ (Präklusivfrist) gemäß § 34 Abs. 1 DSG 2000 gefunden (und der Revision der beklagten Partei (Kreditinstitut) nicht statt gegeben).

Ansprüche nach den §§ 30 bis 32 DSG sind nach dem klaren Wortlaut des § 34 Abs. 1 DSG auch dann präkludiert, wenn nur die einjährige subjektive Frist („Kenntnis von dem beschwerenden Ereignis“) abgelaufen ist.

Aus der gefestigten Rechtsprechung des Lauterkeits- und Schadenersatzrechtes leitet der Oberste Gerichtshof ab, dass bei rechtswidrigen Dauerzuständen (wie die Datenverwendung in einem Informationsverbundsystem ohne Zustimmung bzw. ohne ausreichende Information wie es die Auflagenbescheide der Datenschutzkommission vorsehen) sowohl die subjektive einjährige als auch die objektive dreijährige Präklusivfrist nicht vor Beendigung dieses Dauerzustands beginnt.

Hintergrund: Die Klägerin hatte 2005 einen Abstattungskredit bei der beklagten Partei in Höhe von EUR 6.300,-- aufgenommen. Im Rahmen einer Schuldenregulierung wurde die letzte Rate im Juni 2013 zurückgezahlt. Der KKE–Eintrag umfasste neben den Stammdaten und der Kredithöhe das Datum der Mahnung, Fälligstellung und Klagseinreichung (2007/2008). Aufgrund der Eintragungen in der KKE wurden der Klägerin Kreditverträge von anderen Kreditinstituten verweigert.

4 https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20170529_OGH0002_0060OB00217_16D0000_000

Die Verwendung der Daten entgegen den Bestimmungen des DSG erfolgte, da die Klägerin nicht ausreichend über die Gründe zur Eintragung in die KKE, die Natur des Informationsverbundsystems sowie über die Art der Weitergabe und die Rechtsbehelfe informiert worden sei (unter ausdrücklicher Bezugnahme auf den Auflagenbescheid der Datenschutzkommission zur Registrierung der Kleinkreditevidenz).

4.3 Verwaltungsgerichtshof

4.3.1 VwGH, Ro 2016/04/0051, 23. Oktober 2017

Ein Unternehmen suchte bei der Datenschutzkommission (jetzt: Datenschutzbehörde (DSB)), um Registrierung einer Videoüberwachung für seine Unternehmenszentrale an. Gemäß § 50c Abs. 1 DSG 2000 verlangte die Behörde die Vorlage einer Betriebsvereinbarung, die gemäß § 96a des Arbeitsverfassungsgesetzes 1974 (ArbVG) abgeschlossen werden müsse. § 96a ArbVG sieht nämlich vor, dass der Betriebsrat in Form einer Betriebsvereinbarung zustimmen muss, wenn Kameras, mit der auch Arbeitnehmer gefilmt werden, im Betrieb eines Unternehmens installiert werden. Da das Unternehmen keine solche Betriebsvereinbarung vorlegte, lehnte die (zuständig gewordene) DSB die Registrierung mit Bescheid ab.

Das Unternehmen erhob dagegen Beschwerde beim Bundesverwaltungsgericht (BVwG). Das BVwG wies die Beschwerde ab und begründete dies – wie schon die DSB – damit, dass das Unternehmen eine Betriebsvereinbarung gemäß § 96a ArbVG abschließen und vorlegen müsse. Weiters führte das BVwG aus, dass eine mündliche Verhandlung entfallen könne, weil eine solche vom Unternehmen auch nicht beantragt worden sei.

Das Unternehmen erhob gegen das abweisende Erkenntnis des BVwG eine Revision an den Verwaltungsgerichtshof (VwGH).

Der VwGH sprach in seinem Erkenntnis aus, dass das BVwG und die DSB als Vorfrage beurteilen muss, ob eine Betriebsvereinbarung gemäß § 96a ArbVG abzuschließen und in Folge gemäß § 50c Abs. 1 DSG 2000 im Registrierungsverfahren vorzulegen ist. Der VwGH sagte weiters, dass es bei der Frage, ob gemäß § 96a ArbVG eine Betriebsvereinbarung abzuschließen ist, wenn im Betrieb Kameras installiert werden, mit der auch Arbeitnehmer gefilmt werden, nicht darauf ankommt, ob das Unternehmen mittels Videoüberwachung Arbeitnehmer überwachen will, sondern ob die Videoüberwachung „objektiv“ dazu geeignet ist, Mitarbeiter zu kontrollieren. Da letzteres der Fall ist, muss eine Betriebsvereinbarung gemäß § 96a ArbVG abgeschlossen werden. Das BVwG bzw. die DSB hätten hier also richtig entschieden.

Trotzdem hob der VwGH aber das Erkenntnis des BVwG auf: Das Unternehmen hat die Einvernahme mehrerer Zeugen beantragt. Das BVwG wertete dies aber nicht als Antrag auf Durchführung einer mündlichen Verhandlung und führte daher keine mündliche Verhandlung durch. Darin lag ein Verfahrensfehler, der der Revision schließlich zum Erfolg verhalf.

4.3.2 VwGH, Ra 2017/04/0030, 11. Mai 2017 und VwGH, Ra 2016/04/0144, 5.April 2017

Beiden Entscheidungen des VwGH lag zugrunde, dass zunächst ein Beschwerdeführer (Bf) bei der DSB eine Beschwerde wegen Verletzung seines Rechts auf Geheimhaltung persönlicher Daten eingebracht hatte. Die Datenschutzbehörde wies beide Beschwerden jeweils mit Bescheid ab.

Beide Bf erhoben gegen die abweisenden Bescheide der DSB Beschwerde beim BVwG. Das BVwG hielt in seinen Verfahren jeweils keine mündlichen Verhandlungen ab. In Folge hob das BVwG die Bescheide der DSB mittels Beschluss auf und verwies die Sache zurück an die DSB. Das BVwG begründete seine Entscheidungen jeweils damit, dass die Sachverhaltsfeststellungen der DSB gravierend mangelhaft gewesen seien.

Die DSB erhob gegen die - die Bescheide der DSB jeweils aufhebenden - Beschlüsse des BVwG Revision an den VwGH.

In beiden Fällen hob nun seinerseits der VwGH die Beschlüsse des BVwG wegen Rechtswidrigkeit des Inhalts auf und begründete dies damit, dass das BVwG die seiner Meinung nach fehlenden Sachverhaltsfeststellungen (im ersten Fall zur Frage, ob der Bf ein ärztliches Schreiben in einem verschlossenen oder unverschlossen Kuvert an seinen Arbeitgeber übergeben habe und im zweiten Fall zur Frage, ob der Bf für die Datenempfängerin identifizierbar gewesen sei bzw ob am Tag der behaupteten Datenübermittlung ein Anrufbeantworter in Betrieb gewesen sei) leicht selbst - in einer mündlichen Verhandlung - hätte treffen können. Das BVwG hätte also jeweils selbst eine inhaltliche Entscheidung treffen müssen und nicht den Fall wieder an die DSB zurückverweisen dürfen.

4.4 Europäischer Gerichtshof für Menschenrechte

4.4.1 EGMR, 27.06.2017 - 931/13

Bereits am 21. Juli 2015 entschied der Europäische Gerichtshof für Menschenrechte erstmalig in der Rechtssache Satakunnan Markkinapörssi Oy und Satamedia Oy gegen Finnland. Nunmehr bestätigte die Große Kammer ihr Urteil von vor zwei Jahren, indem sie zum Schluss kam, dass das Recht auf Meinungs- und Informationsfreiheit nicht verletzt wurde. Mit fünfzehn zu zwei Stimmen befand die Große Kammer, das Verbot seitens der finnischen Datenschutzbehörde, welche zwei Medienunternehmen untersagt hatte, persönliche Steuerdaten in der Art und Weise und in dem Umfang zu veröffentlichen, in denen sie solche Daten früher veröffentlicht hatte, sei als rechtmäßiger, legitimer und notwendiger Eingriff in das Recht der Beschwerdeführer auf Meinungs- und Informationsfreiheit zu betrachten. Der EGMR bestätigte den Ansatz der finnischen Behörden, die den Einwand der Beschwerdeführer abgelehnt hatten, es gelte die Ausnahme für journalistische Tätigkeit vom Gesetz zum Schutz personenbezogener Daten.

Der EGMR stellte fest, den Kern des vorliegenden Falls bilde die Frage, ob eine korrekte Abwägung zwischen dem Recht auf Meinungs- und Pressefreiheit nach Artikel 10 EMRK einerseits und dem Recht auf Privatsphäre nach Artikel 8 EMRK andererseits vorgenommen wurde (beide Rechte seien gleichermaßen zu würdigen). Zudem verwies der EGMR auf eine Reihe von Grundsätzen in Bezug auf Pressfreiheit sowie in Bezug auf den Schutz der Privatsphäre, wobei er unterstrich, dass „die Tatsache, dass Informationen bereits gemeinfrei sind, nicht unbedingt den Schutz nach Artikel 8 der Konvention aufhebt“. Der EGMR war der Auffassung, der fragliche Eingriff sei gesetzlich vorgesehen gewesen und habe das legitime Ziel des Schutzes des Ansehens oder der Rechte Dritter verfolgt.

Es bleibt jedoch die Frage, ob der Eingriff in einer demokratischen Gesellschaft notwendig war. Da die beklagte Veröffentlichung nicht als Beitrag zu einer Diskussion von öffentlichem Interesse und auch nicht als Form politischer Rede betrachtet werden könne, könne sie nicht von der privilegierten Stellung solcher Rede profitieren, was den EGMR zu größter Genauigkeit in Bezug auf Eingriffe in die Pressefreiheit anhalte und wenig Spielraum für Einschränkungen

nach Art. 10 Abs. 2 EMRK erlaube. Die überwiegende Mehrheit der Großen Kammer schloss sich der Erkenntnisse auf nationaler Ebene an, „dass die Veröffentlichung der Steuerdaten in der beschriebenen Art und Weise sowie in dem Umfang keinen Beitrag zu einer Diskussion von öffentlichem Interesse geleistet hat und dass die Beschwerdeführer nicht substanziell nachweisen konnten, dass dies allein zu journalistischen Zwecken im Sinne des inländischen und des EU-Rechts erfolgt ist".

Der EGMR kam folglich zu dem Schluss, die finnischen Behörden hätten im „Ermessensspielraum" gehandelt, als sie eine gerechte Abwägung zwischen den widerstreitenden Interessen vornahmen. Somit liege kein Verstoß gegen Artikel 10 EMRK vor. Die Große Kammer bestätigte andererseits die Feststellung eines Verstoßes gegen Art. 6 Abs. 1 EMRK (Recht auf ein faires Verfahren), da die Dauer des Verfahrens auf nationaler Ebene (sechs Jahre und sechs Monate) übermäßig gewesen sei.

4.5 Europäischer Gerichtshof

4.5.1 C-398/15 (Manni) Urteil vom 9. März 2017

Salvator Manni ist gegenwärtig alleiniger Geschäftsführer des Bauunternehmens Italiana Costruzioni Srl. In dieser Eigenschaft verklagte er die Handelskammer, weil aus dem von der Handelskammer geführten Handelsregister hervorgehe, dass er früher alleiniger Geschäftsführer und Liquidator des Unternehmens Immobiliare e Finanziara Srl gewesen sei. Dieses Unternehmen wurde 1992 insolvent erklärt und im Jahr 1995 aus dem Handelsregister gelöscht. Die vom Handelsregister entnommenen Daten werden von gewerblichen Informationsgesellschaften wie Cerved Spa verarbeitet. Herr Manni begehrte daher beim nationalen Gericht der Handelskammer aufzutragen, die Daten die seinen Namen mit der genannten Insolvenz in Verbindung bringen, zu löschen zu anonymisieren oder zu sperren. Ferner begehrte er von der Handelskammer Ersatz des Imageschadens.

Nach Ansicht des EuGH genügt insoweit die Verarbeitung personenbezogener Daten, die von der mit der Führung des Registers betrauten Stellen in Durchführung von Artikel 2 Abs. 1 Buchst. d und j und Artikel 3 der Richtlinie 68/151 vollzogen wird, den Anforderungen von Artikel 7 lit. c, lit. e, und lit. f der Richtlinie 95/46.

Der EuGH stellte klar, dass die Offenlegung dazu dient, die Interessen Dritter gegenüber Aktiengesellschaften und Gesellschaften mit beschränkter Haftung zu schützen. Die Offenlegung soll es Dritten daher erlauben, sich über die wesentlichen Urkunden der Gesellschaft sowie einige der sie betreffenden Angaben, insbesondere die Personalien derjenigen, die die Gesellschaft verpflichten können zu unterrichten. Ein weiterer Zweck besteht darin, Dritte informieren zu können, ohne dass diese ein schutzbedürftiges Recht oder Interesse nachweisen müssen.

Nach Rechtsansicht des EuGH steht fest, dass auch nach Auflösung einer Gesellschaft Rechte oder Rechtsbeziehungen fortbestehen können, die sich auf diese Unternehmen beziehen. In Anbetracht der Vielzahl der möglichen Szenarien, in denen Akteure in mehreren Mitgliedsstaaten beteiligt sein können, sowie der erheblichen Unterschiede bezüglich der Verjährungsfristen der verschiedenen nationalen Rechtsordnungen für die verschiedenen Rechtsgebiete, erscheint es derzeit nicht möglich, eine einheitliche Frist festzulegen, die mit der Auflösung einer Gesellschaft beginnt und nach deren Ablauf die Eintragung der Daten im Register und ihre Offenlegung nicht mehr notwendig wären.

Die Löschung eines Eintrages kann auf Basis von Art. 14 Abs. 1 lit. a der Richtlinie 95/46 (Widerspruchsrecht) verlangt werden. Dies setzt eine individuelle Interessenabwägung voraus.

Der EuGH stellt allerdings klar, dass die Anwendung von Artikel 14 Abs. 1 lit. a der Richtlinie 95/46 unter dem Vorbehalt steht, dass im einzelstaatlichen Recht keine entgegenstehende Bestimmung vorgesehen ist.

4.5.2 C-13/16 (Rīgas satiksme vs. Nationalpolizei) Urteil vom 4. Mai 2017

Rīgas satiksme (ein lettischer Verkehrsbetrieb) wollte Auskunft über einen schadenverursachenden - zu diesem Zeitpunkt minderjährigen - Taxifahrgast ausschließlich zwecks Erhebung einer Zivilklage von der Nationalpolizei haben. Die Nationalpolizei gab dem Antrag nur teilweise statt und lehnte die Bekanntgabe der persönlichen Identifikationsnummer und des Wohnsitzes ab.

Das Verwaltungsgericht 1. Instanz gab der Klage von Rīgas satiksme statt. Dagegen erhob die Nationalbehörde Kassationsbeschwerde an den Obersten Gerichtshof in Verwaltungsstreitigkeiten, das den EuGH um Vorabentscheidung zur Auslegung des Art 7 Buchst. f der DS-RL ersuchte.

Art. 7 Buchstabe f der Richtlinie 95/46 (DS-RL) lautet:
Die Mitgliedstaaten sehen vor, dass die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist:
f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Abs. 1 geschützt sind, überwiegen.

Der EuGH kommt zu Ergebnis, dass in diesem konkreten Einzelfall der Verursacher des Schadens ohne Anschrift und/oder Identifikationsnummer nicht hinreichend für eine Klage zu identifizieren ist, weshalb diese Angaben erforderlich sind. Weiters ist es nicht gerechtfertigt, die Übermittlung deshalb abzulehnen, weil der Verursacher des Schadens minderjährig ist.

So kommt der EuGH zu folgendem Urteil: Art. 7 Buchst. f der Richtlinie 95/46/EG ist dahin auszulegen, dass er nicht dazu verpflichtet, einem Dritten personenbezogene Daten zu übermitteln, damit er vor einem Zivilgericht eine Klage auf Schadenersatz gegen den Verursacher erheben kann. Jedoch steht er der Übermittlung solcher Daten auf der Grundlage des nationalen Rechts nicht entgegen.

4.5.3 C-434/16 (Peter Nowak gegen Data Protection Commissioner) Urteil vom 20. Dezember 2017

Der Gerichtshof hatte darüber zu entscheiden, ob schriftliche Antworten eines Prüflings in einer berufsbezogenen Prüfung und etwaige Anmerkungen des Prüfers als Informationen über den Prüfling iSv Art. 2 Buchst. a RL 95/46/EG – personenbezogene Daten – zu qualifizieren sind. Zunächst hält dieser fest, dass der Anwendungsbereich der RL sehr weit ist und die von ihr erfassten personenbezogenen Daten sehr vielfältig sind. Dabei ist zu beachten, dass die Antworten eines Prüflings sowohl den Kenntnisstand und das Kompetenzniveau des Prüflings sowie gegebenenfalls seine Gedankengänge, sein Urteilsvermögen und sein kritisches Denken wiedergeben und daher Informationen darstellen, welche mit seiner Person verknüpft sind. Bei handschriftlich verfassten Arbeiten enthalten die Antworten zudem kalligrafische Informatio-

nen. Jedenfalls zielt jede Prüfung darauf ab, die individuelle Leistung des Prüfungsteilnehmers festzustellen und zu dokumentieren.

Auch die Anmerkungen eines Prüfers stellen Informationen über den betreffenden Prüfling dar, weil diese aufgrund ihres Inhalts, Zwecks und Auswirkungen mit dem Prüfling verknüpft sind. Die Einordnung der Antworten und Anmerkungen als personenbezogene Daten kann im Übrigen nicht dadurch beeinflusst werden, dass eine solche Einordnung für den Prüfling – grundsätzlich – ein Recht auf Auskunft und Berichtigung gemäß Art. 12 der RL eröffnet. Dabei hat der Prüfling u.a. ein Interesse daran, dem widersprechen zu können, dass die von ihm gegebenen Antworten und die Anmerkungen des Prüfers ohne seine Zustimmung außerhalb des Prüfungsverfahrens verarbeitet oder an Dritte weitergegeben oder veröffentlicht werden. Folglich kann es Situationen geben, in denen die Rechte auf Auskunft und Berichtigung gerechtfertigt sein können, ebenso wie die Geltendmachung des Rechts auf Löschung (z.B. wenn das Prüfungsverfahren endgültig abgeschlossen ist und keiner Anfechtung mehr zugänglich, sodass Antworten oder Anmerkungen jeden Beweiswert verloren haben).

Der EuGH kommt zu folgendem Ergebnis: Art. 2 Buchst. a der RL 95/46/EG ist demnach dahin auszulegen, dass unter Umständen wie denen des Ausgangsverfahrens die schriftlichen Antworten eines Prüflings in einer berufsbezogenen Prüfung und etwaige Anmerkungen des Prüfers zu diesen Antworten personenbezogene Daten im Sinne dieser Bestimmung darstellen.

.

5 Datenschutz-Grundverordnung und Vorbereitungsmaßnahmen der DSB

Ebenso wie im Jahr 2016 war auch das Jahr 2017 den intensiven Vorbereitungen für das Ingeltungtreten der Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 gewidmet.

Neben zahlreichen Aktivitäten, die die Datenschutzbehörde in ihrem eigenen Wirkungsbereich durchgeführt hat und auf die in Folge eingegangen wird, sind als wichtige Eckpunkte die Verabschiedung des Datenschutz Anpassungsgesetzes 2018 (DSG) sowie dessen Kundmachung im BGBl. I Nr. 120/2017 hervorzuheben.

Das DSG führt einerseits die DSGVO durch, indem es Begleitregelungen enthält und die DSGVO dort, wo es der Unionsgesetzgeber zulässt, präzisiert. Andererseits wird mit dem DSG auch die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (DSRL-PJ) umgesetzt.

Die Datenschutzbehörde hat sich in die Vorbereitungen des DSG eingebracht und im Rahmen der allgemeinen Begutachtung eine umfangreiche Stellungnahme abgegeben, die auf der Website des Parlaments abrufbar ist.

Der vom Bundeskanzleramt-Verfassungsdienst ursprünglich vorgelegte Entwurf, der auch als Regierungsvorlage im Parlament eingebracht wurde und welcher eine verfassungsrechtliche Kompetenzbereinigung in Angelegenheiten des Datenschutzes (Bundeskompetenz in Gesetzgebung und Vollziehung) vorsah, konnte mangels Vorliegen der zur Änderung der Verfassungsbestimmungen notwendigen Mehrheit nicht beschlossen werden. Stattdessen wurde das DSG 2000 umfassend novelliert; das DSG fußt daher auf der Stammfassung des DSG 2000, BGBl. I Nr. 165/1999, die Verfassungsbestimmungen blieben unverändert.

Soweit es die Datenschutzbehörde betrifft, sieht das DSG vor, dass die Datenschutzbehörde die zuständige nationale Aufsichtsbehörde nach der DSGVO und nach der DSRL-PJ sein wird. An der Struktur der Datenschutzbehörde als monokratischer weisungsfreier Behörde, die zugleich Dienstbehörde und Personalstelle ist, wird sich nichts ändern.

Ändern werden sich der Aufgabenbereich der Datenschutzbehörde sowie die ihr eingeräumten Befugnisse.

Die Aufgaben der Datenschutzbehörde ergeben sich unmittelbar aus Art. 57 DSGVO, die Befugnisse aus Art. 58, wobei hier nur die wesentlichsten Aufgaben hervorgehoben werden sollen.

Nach **Art. 57 Abs. 1** lit. f haben sich die Aufsichtsbehörden mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Art. 80 zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und die Ergebnisse des Verfahrens zu unterrichten. Lit. g normiert eine Pflicht zur Zusammenarbeit mit anderen Aufsichtsbehörden und zur Leistung von Amtshilfe. Nach lit. j obliegt den Aufsichtsbehörden die Festlegung von Standardvertragsklauseln für die Heranziehung von

Auftragsverarbeitern, für den Datenverkehr mit Drittstaaten oder Internationalen Organisationen. Lit. k bestimmt, dass die Aufsichtsbehörden eine Liste der Verarbeitungsarten, für die eine Datenschutz-Folgeabschätzung nach Art. 35 durchzuführen ist, zu erstellen und zu führen haben. Die lit. p und q sehen vor, dass die Aufsichtsbehörden Kriterien für die Akkreditierungen von Stellen für die Überwachung der Einhaltung von Verhaltensregeln (Art. 41) und für Zertifizierungsstellen (Art. 43) abzufassen und zu veröffentlichen sowie die Akkreditierungen vorzunehmen haben.

Art. 57 Abs. 2 bestimmt, dass die Aufsichtsbehörden entsprechende Musterformulare bereitzustellen haben, um Eingaben an sie zu erleichtern.

Abs. 3 normiert die grundsätzliche Gebührenbefreiung für Betroffene und für Datenschutzbeauftragte, wenn diese sich mit Eingaben an eine Aufsichtsbehörde wenden.

Abs. 4 legt ein Ablehnungsrecht der Aufsichtsbehörden fest. Demnach kann eine Aufsichtsbehörde bei offenkundig unbegründeten oder exzessiven Anfragen eine angemessene Bearbeitungsgebühr verlangen oder sich weigern, tätig zu werden. Die Beweislast hiefür trägt die Aufsichtsbehörde.

Art. 58 DSGVO unterscheidet zwischen Untersuchungsbefugnissen (Abs. 1), Abhilfebefugnissen (Abs. 2), Genehmigungsbefugnissen und beratenden Befugnissen (Abs. 3).

Als Untersuchungsbefugnisse werden u.a. die Anweisung, Informationen bereitzustellen, sowie der Zugang zu Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und –geräte, genannt.

Als Abhilfebefugnisse nennt Abs. 2 insbesondere:
- die Möglichkeit Warnungen und Verwarnungen auszusprechen
- Aufträge an Verantwortliche und Auftragsverarbeiter zu erteilen, gewisse Handlungen vorzunehmen, um Rechten von Betroffenen zu entsprechen oder Verarbeitungsvorgänge in Einklang mit der DSGVO zu bringen
- die Verhängung von Geldbußen nach Art. 83 zusätzlich zu oder anstelle einer anderen Abhilfemaßnahme

Abs. 3 nennt als Genehmigungsbefugnisse bzw. beratende Befugnisse unter anderem
- die Genehmigung von Verhaltensregeln nach Art. 40
- die Akkreditierung von Zertifizierungsstellen bzw. Stellen zur Überwachung der Einhaltung von Verhaltensregeln
- die Genehmigung bestimmter Vertragsklauseln im Hinblick auf Datenübermittlungen an Empfänger in einem Drittstaat oder an eine internationale Organisation

Damit einhergehend hat die Datenschutzbehörde 16 zusätzliche Planstellen beantragt, um die Vollziehung der zusätzlichen Aufgaben und Befugnisse zu gewährleisten. Eine endgültige Entscheidung darüber, ist im Berichtsjahr nicht gefallen.

Die Datenschutzbehörde hat im eigenen Wirkungsbereich zur Vorbereitung auf diese Änderungen folgende Maßnahmen im Berichtsjahr ergriffen:
- Interne Schulungen für Bedienstete der Datenschutzbehörde
- Regelmäßige Beiträge im Newsletter der Datenschutzbehörde zur DSGVO
- Bereitstellung wesentlicher Informationen zur DSGVO auf der Website der Datenschutzbehörde, welche regelmäßig aktualisiert werden (insbesondere „Leitfaden zur DSGVO“, in dem die DSGVO kurz und übersichtlich dargestellt wird und häufig gestellte Fragen beant-

wortet werden, sowie beschlossene „Leitlinien der Art. 29-Gruppe“)
- Verstärkte Teilnahme auf europäischer Ebene an maßgeblichen Untergruppen der Art. 29-Gruppe
- 5 Informationsveranstaltungen für Bundes- und Landesbehörden (vier in Wien, eine in Salzburg)
- Regelmäßiger Kontakt zu Plattformen betrieblicher und behördlicher Datenschutzbeauftragter
- Durchführung von zwei Planspielen zur Vorbereitung auf grenzüberschreitende Sachverhalte und die internationale Zusammenarbeit mit Partnerbehörden
- Teilnahme von Bediensteten der Datenschutzbehörde an Sitzungen und Konferenzen, die der DSGVO gewidmet sind
- mehr als 50 Vorträge von Bediensteten der Datenschutzbehörde in zahlreichen Foren (u.a. berufliche Interessens- und Standesvertretungen, Universitäten, Verwaltungsakademien der Länder etc.)
- Zuteilung von vier Bediensteten der Datenschutzbehörde zu verschiedenen Verwaltungsstrafbehörden zur Vorbereitung auf die Durchführung von Verwaltungsstrafverfahren
- Absolvierung von Englischkursen durch Bedienstete der Datenschutzbehörde (zur Vorbereitung auf grenzüberschreitende Verfahren und internationale Kooperation)
- Mitwirkung von Bediensteten der Datenschutzbehörde an Kommentaren und Beiträgen zur DSGVO und zum DSG

6 Europäische Zusammenarbeit

6.1 Europäische Union

6.1.1 DIE ART. 29 DATENSCHUTZGRUPPE

Diese nach Art. 29 der Datenschutz-Richtlinie benannte Gruppe ist das Forum sämtlicher Datenschutzbehörden des EWR. Mit 25. Mai 2018 wird die Art. 29-Datenschutzgruppe im Zuge des In-Geltung-Tretens der DSGVO im Europäischen Datenschutzausschuss aufgehen und sodann als Einrichtung der Europäischen Union über eigene Rechtspersönlichkeit verfügen.

Die Gruppe tagt in etwa sechsmal pro Jahr im Plenum, wobei an diesen Sitzungen im Regelfall die jeweiligen Behördenleiter, der Europäische Datenschutzbeauftragte sowie Experten der Europäischen Kommission teilnehmen.

Zur Vorbereitung dieser Sitzungen sowie zur Vorbereitung von zu beschließenden Dokumenten sind diverse Untergruppen (Subgroups) eingerichtet, die sich mit sektorspezifischen Fragen des Datenschutzes auseinandersetzen.

Im Zusammenhang mit der Umsetzung der DSGVO sowie der Rechtsdurchsetzung im Bereich des Angemessenheitsbeschlusses der Europäischen Kommission betreffend die USA (Privacy Shield; Durchführungsbeschluss (EU) 2016/1250) haben Bedienstete der DSB im Jahr 2017 an zahlreichen Sitzungen der Untergruppen der Art. 29-Gruppe teilgenommen. Der Fokus lag dabei insbesondere darauf, den Übergang auf den neuen Rechtsrahmen bestmöglich vorzubereiten.

Dazu wurden von der Art. 29-Gruppe im Jahr 2017 folgende Leitlinien vorbereitet, die auf der Website der Europäischen Kommission (teilweise auch schon in allen Amtssprachen der EU) abrufbar sind:

- Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679
- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679
- Guidelines on Personal data breach notification under Regulation 2016/679
- Guidelines on Consent under Regulation 2016/679
- Guidelines on Transparency under Regulation 2016/679
- Leitlinien zum Recht auf Datenübertragbarkeit
- Leitlinien in Bezug auf Datenschutzbeauftrage
- Leitlinien für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters
- Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“

Die bereits in deutscher Übersetzung vorliegenden Leitlinien und die „Guideline on the application and setting of administrative fines“ sind unter anderem auch direkt auf der Website der DSB abrufbar.

Bei den von der DSB beschickten Untergruppen der Art. 29-Gruppe handelt es sich um
a. die Cooperation Subgroup
b. die Key Provisions Subgroup
c. die Future of Privacy Subgroup
d. die Technology Subgroup
e. die International Transfer Subgroup
f. die Financial Matters Subgroup
g. die Border, Travel and Law Enforcement Subgroup

Daneben leitet und koordiniert die Datenschutzbehörde die E-Government-Subgroup.

Zu den einzelnen Untergruppen im Detail.
a. Cooperation Subgroup
Diese Untergruppe dient der Vorbereitung auf die in Kapitel VII DSGVO vorgesehene grenzüberschreitende Kooperation zwischen den Datenschutzbehörden sowie der Vorbereitungen auf den Europäischen Datenschutz-Ausschuss, der die Art. 29-Gruppe ablösen wird.

b. Key Provisions Subgroup
Diese Untergruppe befasst sich, unvorgreiflich einer rechtsverbindlichen Auslegung durch den EuGH, mit ausgewählten Begriffen der DSGVO und deren Interpretation.

Diese Untergruppe hat 2017 die Ende 2016 vom Plenum beschlossene Leitlinien (Guidelines on Data Protection Officers, WP 243, Guidelines for identifying a controller or processor's lead supervisory authority, WP 244), die die Bestimmungen der DSGVO betreffend Datenschutzbeauftragte (Art. 37 bis 29 DSGVO) und die Bestimmung der federführenden Aufsichtsbehörde (Art. 56 DSGVO) erläutern, überarbeitet. Diese wurden vom Plenum in der 1. Jahreshälfte 2017 angenommen. Von beiden Leitlinien liegen inzwischen auch Übersetzungen in die deutsche Sprache vor, die u.a. auch auf der Website der DSB verlinkt abgerufen werden können.

2017 neu erstellt und im Oktober 2017 vom Plenum angenommen wurden Leitlinien (Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679; WP 251), die automatisierte Entscheidungen im Einzelfall einschließlich Profiling gemäß Art. 22 DSGVO erläutern.

c. Future of Privacy (FoP) Subgroup
Diese Untergruppe, in der in erster Linie die Leiter der jeweiligen Datenschutzbehörden vertreten sind, bereitet strittige Fragen für das Plenum der Art. 29-Gruppe auf und dient zudem der Klärung grundsätzlicher Fragen zu Entwicklungen im Datenschutzrecht.

d. Technology Subgroup
Diese Untergruppe befasst sich mit Technologien und deren Auswirkungen auf den Datenschutz, ua. Drohnen oder Cookie-Technologie. Die Untergruppe hat im Berichtszeitraum den Übergang zur Datenschutz-Grundverordnung vorbereitet ua. zum Recht auf Datenübertragbarkeit (Art. 20 DSGVO) und zur Datenschutz-Folgenabschätzung (Art. 35 DSGVO).

e. International Transfer Subgroup
Diese Untergruppe beschäftigt sich hauptsächlich mit Angelegenheiten des internationalen Datenverkehrs – demnach mit Datenübertragungen von der EU in Drittstaaten. Dabei ist insbesondere die Befassung mit Fragen, Maßnahmen und Regelungen im Zusammenhang mit dem EU-US-Datenschutzschild erwähnenswert. Außerdem wurde im vergangenen Jahr inten-

siv an den wesentlichen Arbeitspapieren der Art-29 Datenschutzgruppe betreffend „Binding Corporate Rules“ (BCRs) – verbindliche interne Datenschutzvorschriften – und deren Adaptierung an die Vorgaben gemäß der Datenschutzgrundverordnung gearbeitet.

f. Financial Matters Subgroup
Die Untergruppe beschäftigte sich mit datenschutzrechtlichen Fragen im Bereich des Zoll-, Bank- und Steuerwesens. Die wesentlichen europarechtlichen Fragen betreffend die Zahlungsdienste-Richtlinie („PSD II“) sowie „Administrative Arrengement“ betreffend die Übermittlung von personenbezogenen Daten zwischen Finanzmarkt-Aufsichtsbehörden der EU-Mitgliedstaaten und von nicht EU-Mitgliedstaaten.

g. BTLE
Die Borders Travel & Law Enforcement Untergruppe beschäftigte sich 2017 beispielsweise mit Fragen der Einführung zur „e-evidence“, ein diesbezüglicher Vorschlag ist durch die Kommission Anfang 2018 geplant. Die Untergruppe beschäftigte sich auch mit einem Vorschlag zum Arbeitsdokument „Future of Supervision Models“, der Anfang 2018 konkretisiert werden soll. Darüber hinaus beschäftigte man sich erneut mit der Umsetzung der Datenschutz-Richtlinie für Polizei und Strafjustiz (Richtlinie (EU) 2016/680), eine diesbezügliche Leitlinie steht im Laufe von 2018 im Raum.

6.1.2 Europol

Das Europäische Polizeiamt (Europol) ist eine europäische Polizeibehörde mit der Aufgabe, die Leistungsfähigkeit der zuständigen Behörden der Mitgliedstaaten und ihre Zusammenarbeit im Hinblick auf die Verhütung und die Bekämpfung des Terrorismus, des illegalen Drogenhandels und sonstiger schwerwiegender Formen der internationalen Kriminalität zu verbessern. Europol verarbeitet zu diesem Zweck große Mengen von vor allem strafrechtsrelevanten Daten. Diese Verarbeitung unterlag bis Mai 2017 der besonderen Kontrolle durch eine gemeinsame Kontrollinstanz, die aus Vertretern aller EU Datenschutzbehörden bestand, dem „Europol Joint Supervisory Body“ (JSB). Mit der Europol Verordnung[5] 794/2016 vom 11. Mai 2016, die am 01.Mai 2017 in Kraft trat, wurde diese gemeinsame Kontrollinstanz abgeschafft. An ihre Stelle trat eine geteilte Kontrolle: Einerseits die nationalen Kontrollinstanzen, die die Zulässigkeit der Eingabe und des Abrufs personenbezogener Daten sowie jedweder Übermittlung dieser Daten an Europol überwachen und andererseits der europäische Datenschutzbeauftragte (EDPS), der die Verarbeitung durch Europol überwacht. Jede betroffene Person kann beim Europäischen Datenschutzbeauftragten eine Beschwerde einreichen, wenn sie der Ansicht ist, dass Europol bei der Verarbeitung ihrer personenbezogenen Daten gegen die Europol-Verordnung verstößt. Darüber hinaus kann jede Person die nationale Kontrollbehörde ersuchen, die Rechtmäßigkeit jeglicher Übermittlung ihrer personenbezogenen Daten an Europol sowie die Verarbeitung dieser Daten durch den betreffenden Mitgliedstaat zu prüfen. Die Vertreter der nationalen Kontrollbehörde der Mitgliedstaaten und der Europäische Datenschutzbeauftragte bilden gemeinsam den Beirat für Zusammenarbeit. Die Hauptaufgabe des Beirates ist es, sich mit den allgemeinen Richtlinien und Strategien Europol im Bereich der Überwachung des Datenschutzes sowie der Zulässigkeit der Verarbeitung und die Übermittlung von personenbezogenen Daten an Europol auseinanderzusetzen.

6.1.3 Schengen

Das Schengener Informationssystem der zweiten Generation (kurz „SIS II“) ermöglicht nationalen Grenz-, Zoll-, Visa- und Strafverfolgungsbehörden Fahndungen zu gesuchten oder vermissten Personen bzw. gestohlenen oder verlorenen Sachen, insbesondere Dokumente und

5 http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0794&from=EN

Fahrzeuge, im Schengen-Raum auszuschreiben und abzufragen. Die Rechtsgrundlage für das SIS II bildet die SIS-II-Verordnung. [6] Das SIS II besteht aus einem zentralen System (C.SIS), den jeweiligen nationalen Systemen der Mitgliedstaaten (N.SIS II) sowie einer Kommunikationsinfrastruktur zwischen dem zentralen System und den nationalen Systemen. Das österreichische N.SIS II wird vom Bundesministerium für Inneres als datenschutzrechtlich Verantwortlichen geführt. Die jeweiligen nationalen Datenschutzbehörden haben gemäß der SIS-II-Verordnung die Rechtmäßigkeit der Verarbeitung personenbezogener SIS-II-Daten auf nationaler Ebene zu überwachen. Darüber hinaus haben die nationalen Datenschutzbehörden mindestens alle vier Jahre die Datenverarbeitungsvorgänge im N. SIS II nach internationalen Prüfungsstandards zu überprüfen. Im Jahr 2017 hat die Datenschutzbehörde – gemeinsam mit zwei technischen Sachverständigen – ein amtswegiges Prüfverfahren mit einem Schwerpunkt auf die technische Ausgestaltung des N.SIS II durchgeführt. Darüber hinaus überprüft die Europäische Kommission gemeinsam mit nationalen Experten die Anwendung der SIS-II-Verordnung in den einzelnen Mitgliedsaaten. Im Berichtszeitraum haben Mitarbeiter der Datenschutzbehörde an Evaluierungen in Dänemark, Schweden, Portugal und Spanien teilgenommen. Die Datenschutzbehörde wird sich auch im Jahr 2018 an Evaluierungen beteiligen.

6.1.4 Zoll

Das gemeinsame Zollinformationssystem (ZIS) dient der Erfassung von Daten von Waren, Transportmittel, natürlichen und juristischen Personen, die im Zusammenhang mit Verstößen gegen das gemeinsame Zoll- und Agrarrecht stehen. Das ZIS ermöglicht einem Mitgliedstaat, der Daten in das System eingegeben hat, einen ZIS-Partner in einem anderen Mitgliedstaat um die Durchführung gezielter Kontrollen zu ersuchen. Zur Gewährleistung eines angemessenen Datenschutzes wurde neben dem Ausschuss gemäß Art. 43 der ZIS-Verordnung [7](„Joint Supervisory Authority of Customs“ („JSA“)) sowie eine Koordinierende Aufsichtsbehörde (CIS Supervision Coordination Group („CIS-SCG“)) eingerichtet, welche aus Vertretern der nationalen Datenschutzbehörden der Mitgliedstaten und dem Europäischen Datenschutzbeauftragten gebildet wird. Im Berichtszeitraum fand eine Sitzung des JSA bzw. der CIS-SCG statt.

6.1.5 Eurodac

Das „Eurodac“-System ermöglicht den zuständigen Behörden der Mitgliedstaaten Asylwerber und andere Personen zu identifizieren, die beim illegalen Überschreiten einer EU-Außengrenze aufgegriffen werden. Anhand der Fingerabdrücke kann ein Mitgliedstaat feststellen, ob ein Fremder in einem anderen Mitgliedstaat Asyl beantragt hat oder ob ein Asylwerber illegal in die EU eingereist ist. Eurodac besteht aus einer von der Europäischen Kommission verwalteten Zentraleinheit und den in den Mitgliedsstaaten zur Abfrage und Befüllung betriebenen nationalen Systemen. Art. 32 der (EU) Verordnung Nr. 603/2013[8]sieht eine koordinierte Aufsicht und jährliche stichprobenartige Prüfung durch die nationale Datenschutzbehörde und die anderen EU Datenschutzbehörden mit dem Europäischen Datenschutzbeauftragten vor.

6.1.6 Visa

Das Visa-Informationssystem (VIS) enthält Daten zu Ausstellungen, Ablehnungen, Annullierungen, Widerrufen und Verlängerungen von Kurzzeit-Visa in den Mitgliedstaaten des Schengen Raums. Die rechtliche Grundlage für das VIS bildet die Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Einrichtung des Visa-Informationssystems (VIS-Verordnung). Das VIS besteht aus einem zentralen Visa-Informationssystem (CS-VIS), einem nationalen System (N-VIS) in jedem Mitgliedstaat und aus einer Kommunikationsinfrastruktur zwischen dem zentralen Visa-Informationssystem und den nationalen

6 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32006R1987
7 http://eur-lex.europa.eu/legal-content/dE/TXT/?uri=celex:31997R0515
8 http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32013R0603

Systemen. Die nationale VIS-Stelle in Österreich ist das Bundesministerium für Inneres. Die jeweiligen nationalen Datenschutzbehörden haben gemäß der VIS-Verordnung die Rechtmäßigkeit der Verarbeitung personenbezogener VIS-Daten auf nationaler Ebene zu überwachen. Darüber hinaus haben die nationalen Datenschutzbehörden mindestens alle vier Jahre die Datenverarbeitungsvorgänge im N.VIS nach internationalen Prüfungsstandards zu überprüfen. Die Europäische Kommission hat im Berichtszeitraum einen Vorschlag zur Novellierung der VIS-Verordnung veröffentlicht. Der Vorschlag sieht insbesondere vor, das Mindestalter der zu erfassenden Personen von 14 auf 6 Jahre herabzusetzen. Im Rahmen der öffentlichen Konsultation hat die Datenschutzbehörde hierzu eine Stellungnahme abgegeben. [9] Darüber hinaus hat die Datenschutzbehörde im Berichtszeitraum die österreichische Vertretungsbehörde in Mexiko inspiziert. Weiters wurde die Information auf der Webseite der Datenschutzbehörde aktualisiert und ein neues Auskunfts-Formular für Betroffene online gestellt.

6.2 Europarat

Die DSB vertritt die Republik Österreich im Ausschuss nach Art. 18 (T-PD) der Datenschutzkonvention des Europarates (EVS Nr. 108; BGBl. Nr. 317/1988). Im Berichtszeitraum fanden von 19. bis 21 Juni die 34. Plenarsitzung und von 22. bis 24. November 2017 die 35. Plenarsitzung des T-PD in Straßburg statt. Die Tagesordnungen sowie die zusammenfassenden Berichte der Sitzungen sind in englischer Sprache unter https://www.coe.int/en/web/data-protection/consultative-committee-tpd/meetings abrufbar.

9 https://ec.europa.eu/home-affairs/content/consultation-lowering-fingerprinting-age-children-visa-procedure-12-years-6-years_en

7 Internationale Beziehungen

7.1 EU-US-Datenschutzschild (Privacy Shield)

Mit 12. Juli 2016 hat die Europäische Kommission den EU-US-Datenschutzschild (EU-US Privacy Shield) angenommen. Diese Angemessenheitsentscheidung löste die frühere Safe-Harbor Regelung ab. Das Datenschutzschild basiert auf einem System der Selbstzertifizierung. Wurde ein Unternehmen zertifiziert, so ist der Datenfluss an dieses Unternehmen grundsätzlich genehmigungsfrei, das heißt, es ist keine Genehmigung der Datenschutzbehörde erforderlich. Das US-Handelsministerium überprüft die Liste der teilnehmenden Unternehmen regelmäßig, um sicherzustellen, dass die Unternehmen die Regeln einhalten, denen sie sich selbst unterworfen haben. Im Hinblick auf die Transparenz, Verwaltung sowie Überwachung des EU-US-Datenschutzschilds bestehen spezifische Überwachungs- und Durchsetzungsmechanismen. Halten Unternehmen die Regeln in der Praxis nicht ein, kommt es zu entsprechenden Sanktionen bzw. folgt die Streichung von der Liste.

Das EU-US-Datenschutzschild bietet klare Schutzvorkehrungen und Transparenzpflichten beim Datenzugriff durch US-Behörden. Demnach ist ein Datenzugriff von Behörden aus Gründen der Rechtsdurchsetzung oder der nationalen Sicherheit nur unter Einhaltung klarer Beschränkungen, Schutzvorkehrungen und Aufsichtsmechanismen gestattet. Alle Personen in der EU erhalten durch das Datenschutzschild Zugang zu Rechtsschutzmechanismen in diesem Bereich. Außerdem wurde eine Ombudsstelle eingerichtet, an die sich EU-Bürger mit Rechtsschutzbegehren, die den Bereich der nationalen Sicherheit betreffen, wenden können.

Darüber hinaus stellt das EU-US-Datenschutzschild einen Schutzmechanismus für die Rechte des Einzelnen zur Verfügung. Ist ein EU-Bürger der Auffassung, dass seine Daten im Rahmen des Datenschutzschilds missbraucht wurden, stehen ihm mehrere Möglichkeiten der Streitbeilegung offen, von denen er Gebrauch machen kann. Idealerweise wird sich das Unternehmen selbst um die Beschwerde kümmern und das Problem lösen. Außerdem steht ein kostenloses Verfahren der alternativen Streitbeilegung zur Verfügung. Einzelpersonen können sich auch an ihre nationalen Datenschutzbehörden wenden, die dann zusammen mit der US-Handelskommission dafür sorgen, dass Beschwerden nachgegangen und abgeholfen wird. Kann der Fall nicht auf andere Weise gelöst werden, gibt es als letztes Mittel ein Schiedsverfahren. Für Rechtsschutzbegehren von EU-Bürgern, die den Bereich der nationalen Sicherheit betreffen, ist die von den US-Nachrichtendiensten unabhängige Ombudsstelle zuständig.

Daneben wird im Rahmen des EU-US-Datenschutzschilds auch ein jährlicher Überprüfungsmechanismus bereitgestellt. Dabei wird die Funktionsweise des Datenschutzschilds einschließlich der Zusicherungen und Zusagen hinsichtlich des Datenzugriffs aus Gründen der Rechtsdurchsetzung oder der nationalen Sicherheit überwacht. Im September 2017 fand der erste jährliche „Joint Review“ unter Beteiligung von Experten seitens der EU-Kommission, der Art. 29-Datenschutzgruppe sowie seitens der US-amerikanischen Regierung in Washington statt. Insbesondere die Robustheit des Datenschutzschilds sollte dabei bewertet werden. Unter Bezugnahme auf die in den bisherigen Stellungnahmen der Art. 29-Datenschutzgruppe (WP 237, WP 238) angeführten Bedenken wurden sowohl die kommerziellen Aspekte als auch die Teile betreffend die nationale Sicherheit näher beleuchtet. Die wesentlichen Erkenntnisse und Beurteilungen wurden anschließend in einem Bericht der Art. 29-Datenschutzgruppe zusammengefasst, welcher im Newsroom der Art. 29-Datenschutzgruppe abrufbar ist. Unabhängig davon verfasste auch die EU-Kommission einen entsprechenden Bericht zum gegenständlichen „Joint Review“.